Connection Robustness for Wireless Moving Networks

Using Transport Layer Multi-homing

By:

Peyman Behbahani

Under Supervision of Dr Veselin Rakocevic

A THESIS SUBMITTED TO THE SCHOOL OF ENGINEERING AND MATHEMATICAL SCIENCES, CITY UNIVERSITY, LONDON IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF

Doctor of Philosophy

London, UK, Oct. 2010

Abstract

Given any form of mobility management through wireless communication, one useful enhancement is improving the reliability and robustness of transport-layer connections in a heterogeneous mobile environment. This is particularly true in the case of mobile networks with multiple vertical handovers. In this thesis, issues and challenges in mobility management for mobile terminals in such a scenario are addressed, and a number of techniques to facilitate and improve efficiency and the QoS for such a handover are proposed and investigated. These are initially considered in an end-to-end context and all protocols and changes happened in the middleware of the connection where the network is involved with handover issues and end user transparency is satisfied.

This thesis begins by investigating mobility management solutions particularly the transport layer models, also making significant observation pertinent to multi-homing for moving networks in general. A new scheme for transport layer tunnelling based on SCTP is proposed. Consequently a novel protocol to handle seamless network mobility in heterogeneous mobile networks, named nSCTP, is proposed. Efficiency of this protocol in relation to QoS for handover parameters in an end-to-end connection while wired and wireless networks are available is considered. Analytically and experimentally it has been proved that this new scheme can significantly increase the throughput, particularly when the mobile networks roam frequently. The detailed plan for the future improvements and expansion is also provided.

Acknowledgements

First, I would like to thank my supervisor, Dr Veselin Rakocevic. I could not have produced this work without the constant impetus to succeed, support and guidance given by him.

Next, I would like to thank my sponsoring company, T-Systems and particularly BIT (Broadband wireless Internet access in public Transport) project manager, Prof. J. Habermann, who not only funded my research but provided interesting insights and opportunities for interaction with industrial representatives, I am most grateful for this.

Also, thanks to Professor Panos Liatsis my second supervisor and member of Mobile Network Research Group specially Dr Muttukrishnan Rajarajan, Ehsan Hamadani and Soroush Jahromizadeh that I couldn't have achieved this without them. Particular thanks must be given to Professor Abdol-Hamid Aghvami director of Centre for Telecommunications Research (CTR) and its members specially Mohammad Ghavami, Oliver Holland, Nima Nafisi, Reza Dilmaghani, Vasilis Friderikos, Reza Nakhai and Mona Ghassemian that have partaken in some very useful discussions and finally Dominic Stiles for his valuable editorial remarks.

Last but not least, I would like to thank my family and particularly my parents for all the hope, strength and support they have given me throughout this PhD.

List of Acronyms and Abbreviations

Acronym/Abbreviation	Description
2G	2nd Generation
3G	3rd Generation
3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
ACK	ACKnowledgement
AMPS	American Mobile Phone Systems
AP	Access Point
AR	Access Router
ASCONF	Address Configuration Change Chunk
ATM	Asynchronous Transfer Mode
b	Binary Digits (Bits)
B	Bytes
BIT	Broadband wireless Internet access in public Transport
BR	Bridge Router
BU	Binding Update
BWA	Broadband Wireless Access
CDMA-2000	Code Division Multiple Access Ver. 2000
CN	Correspondent Node
CN	Core Network
cwnd	Congestion Window
CoA	Care of Address
CS	Circuit Switched
CSCF	Call State Control Function
DAR	Dynamic Address Reconfiguration
DHCP	Dynamic Host Configuration Protocol
DSL	Digital Subscribe Line
DVB	Digital Video Broadcasting
DVB-AR	Digital Video Broadcasting Access Router
DVB-H	Digital Video Broadcasting - Handheld
FA	Foreign Agent
FDD	Frequency Division Duplex
FEC	Forward Error Correction
FTP	File Transport Protocol
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global Systems for Mobile Communication
H/O Entity	Handover Entity
HA	Home Agent

Acronym/Abbreviation	Description
HIP	Host Identity Payload
HIT	Handover Initiation Time
HMIPv6	Hierarchical Mobile IP version 6
HSS	Home Subscriber Server
I-CSCF	Interrogating Call State Control Function
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISP	Internet Service Provicer
LAN	Local Area Network
LFN	Local Fixed Node
LLC	Logical Link Control
LMN	Local Mobile Node
MAC	Media Access Control
MAN	Metropolitan Area Network
MAP	Mobility Anchor Points
MCoA	Multiple Care of Addresses
ME	Mobile Equipment
MH	Mobile Host
MIP	Mobile IP
MIPv4	Mobile IP version 4
MIPv6	Mobile IP version 6
MN	Mobile Node
MPEG	Motion Pictures Experts Group
MPEG-TS	MPEG Transport Stream
MR	Mobile Router
MR-HA	Mobile Router-Home Agent
MSC	Mobile Switching Centre
mSCTP	Mobile Stream Control Transmission Protocol
MTU	Maximum Transmission Unit
Node B	Node B (UMTS Basestation)
NAD	Network Access Device
NAI	Network Access Identifier
NAT	Network Address Translation/Translator
NEMO	Network Mobility
NMT	Nordic Mobile Telephone Systems
NS-2	Network Simulator Version 2
nSCTP	NEMO Stream Control Transmission Protocol
ORC	Optimised Route Cache Management Protocol
OSI	Open Systems Interconnection Basic Reference Model
PAN	Personal Area Network
P-CSCF	Proxy Call State Control Function

Acronym/Abbreviation	Description
PPP	Packet Pair Probing
PS	Packet Switched
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RAS	Remote Access Service
RFC	Request For Comments
RNC	Radio Network Controller
RNS	Radio Network Subsystem
RO	Route Optimization
RRM	Radio Resource Management
RWP	Random WayPoint
SACK	Selective ACK
S-CSCF	Serving Call State Control Function
SCTP	Stream Control Transmission Protocol
SCTP/IP	Stream Control Transmission Protocol / Internet Protocol
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
SLS	Service Level Subscription
SSN	Stream Sequence Number
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/ Internet Protocol
TDD	Time Division Duplex
TSN	Transmission Sequence Number
UDP	User Datagram Protocol
UE	User Equipment
UMTS	Universal Mobile Telecommunications Service
UMTS-AR	Universal Mobile Telecommunications Service Access Router
USIM	User Services Identify Module
UTRAN	UMTS Terrestrial Radio Access Network
VMN	Visiting Mobile Node
VPN	Virtual Private Network
W-CDMA	Wideband Code Division Multiple Access
Wi-Fi	Wireless Fidelity
WiMAX	World Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WLAN-AR	Wireless LAN Access Router
WMAN	Wireless Metropolitan Area Network

Table of contents

List of figures

List of Tables

Chapter 1. Introduction

As integrated circuit transistor density continues to improve according to Moore's law and operating voltages and power dissipation are cut, more and more terminal functionalities are being implemented. For example, the integration between mobile modem chipsets and WLAN modules is becoming possible, offering connectivity to WLANs as well as to existing cellular networks and featuring compatibility with 802.11b and 802.11g protocols on both CDMA2000 and WCDMA (UMTS) networks. In a wireless access infrastructural point of view, a wide selection of technologies is available in many places throughout the globe. Often, these technologies are designed to fulfil dissimilar purposes, or to provide substitute levels of QoS to users, perhaps with alternative pricing structures. If users were allowed to use or switch between these technologies, dependent on changes in circumstances such as availability, utilised application, or undertaking the importance of the communication, then overall user satisfaction could be enhanced. And if users were allowed to switch between these technologies based on their mobility, for example to take advantage of a high-bandwidth low-cost service available in a limited area (such as a WLAN hot spot), then perceived service quality would be further improved.

In many situations the mobility of diverse users is matched; for instance, in public transport scenarios a number of users remain in the close proximity during the movement of the transportation vehicle. In Mobile IP (MIP)[1], signalling is required for each of these users upon each change in their topological point of attachment to the Internet. However, if the terminal movements could be dealt with as a group, with all terminals using the same network, the group handover would be much more efficient. In the group mobility scenario, signalling used to handover the network with a single set of messages between network's gateway and the gateway's home network. This is the principle behind the concept of NEtwork MObility (NEMO)[2].

The concept of multi-homing becomes more attractive and is gaining increased interest in the telecom research communities. Multi-homing addresses the

problem of link failures by allowing a transport layer session to bind multiple IP addresses at each end point of communication. This feature provides both endpoints with multiple communication paths and thus, gives them the ability to failover (switch) to an alternate path when a link failure occurs or a minimum required QoS has not been met. The simultaneous connectivity can be achieved in a heterogeneous environment by using multiple ISPs or multiple access technologies, such as cellular networks (e.g. GPRS, UMTS) and wireless LANs and MANs (e.g. 802.11, WiMAX).

The current transport layer protocols, TCP and UDP, do not support multi-homing. TCP allows binding to only one network address at each end of connection. This is the main reason why a new transport-layer protocol, the Stream Control Transmission Protocol (SCTP)[3], is being investigated in this thesis. SCTP allows binding of one transport layer association to multiple IP addresses at each end of the association. SCTP has a built-in failure detection and recovery system, known as failover, which allows associations to dynamically send traffic to an alternate peer IP address when needed. SCTP's failover mechanism is static and does not adapt to application requirements or network conditions.

Furthermore, SCTP provides the multi-streaming functionality. Multi-streaming allows independent delivery among data streams. This means that, the application data can be partitioned into multiple streams. These portions or data chunks are formed inside an SCTP packet and each packet can contain multiple data chunks from different applications. The chunks header contains Transmission Sequence Number (TSN), Stream ID and Stream Sequence Number (SSN) that can provide independent delivery of each stream to the application.

In line with these observations, this thesis presents the design of a new protocol for providing a soft and seamless handover for network mobility and particularly the scenarios with fast moving networks such as where they are used on public transport. Moreover, the interest of the thesis is in increasing the quality of service and connection robustness in an all-IP end to end communication scenario, where no presumptions are made about the capabilities of terminals aside from enhancing the gateways to support multilayer protocols. The

advantage of this type of protocol is a much wider applicability of the solutions; furthermore, this is consistent with expectations for future-generation mobile systems.

1.1. Challenges

From the transport layer point of view three significant technical challenges in reliable connections are: congestion control, effect of irresponsible non-congestion control protocols, and the provision of mobility. They are discussed here.

1.1.1. Congestion Control

Congestion control mechanism operates in the Internet to moderate the transmission rate to fairly share the bottleneck bandwidth. The approach of Transmission Control Protocol (TCP) as the most common transport protocol in the Internet is "additive increase multiple decrease". In any end to end connections such as provided by TCP, congestion control only needs to select the appropriate transmission rate based on congestion on the path between the source and the receiver. However, in reliable multi-homed scenarios, there may be multiple network paths for each source-receiver pairing. Hence significant questions arise: Which source-receiver path would be more appropriate for transmission to be selected? How can this selected path be changed in reaction to dynamic variations in congestion, bandwidth or any other changes in the network circumstances among source-receiver paths?

While in the wired networks all losses are generally due to congestion, over wireless links losses can occur randomly. It is not possible for conventional congestion control entities (e.g. TCP) to distinguish between congestion-related and random losses; indeed, the mistaking of random losses for congestion commonly leads to congestion control greatly underestimating the available bandwidth on a path. Specific techniques are therefore necessary to distinguish between random and congestion-related losses, and solutions might also be employed to mitigate the effects of random losses. Basis of these random losses are due to one of the following issues:

- Interference: Cellular telephone channels are subject to adjacent-cell communications using the same signal frequency. The problem with such interference is that it occupies the same frequency band as the desired communication signal, and has a similar structure.
- Noise: Noise signals have little structure and arise from both human and natural sources. That can increase the error-rate in the air interface during transmission. Error-rate is typically very low in wired media; approximately 10^{-12} in fibre-optics and 10^{-3} in UTP cable, while, in a wireless link it is typically 10^{-1} or 1 error every 10 bits[4].
- Limited Bandwidth: This is the maximum rate at which the transmission medium can carry data. Based on communication theorem stated by Shannon–Hartley [5], the maximum amount of error-free digital data that can be transmitted over a communications channel (e.g., a copper wire or an optical fibre) with a specified bandwidth in the presence of noise. In fibre optics it is more than 10Gbps, and in UTP it is up to 1Gbps. In a wireless link, the maximum is about 100Mbps, and significantly reduced in a mobile scenario due to channel fading and noise conditions[4].
- Mobility: The physical movement of end-hosts between regions covered by different networks and access-points are not experienced in wired technology. Change of IP address is a natural consequence of a movement that required router adaptation and appropriated routing which has not defined in a wired scenario. This can include frequent changes in IP addresses and other problems such as brief disconnectivity (blackout) and break-up in data transmission during handover.

1.1.2. Effect of Irresponsible Non-congestion Control Protocols

As mentioned in the previous section, the congestion control mechanism tries to moderate transmission rate, particularly in the bottleneck of the transmission connection and in the case of a combination of wired and wireless scenarios mostly via wireless hops. At the same time the irresponsible non-congestion control transmission protocol (e.g. UDP) is sending the datagrams over the

communication links regardless of consideration of the available bandwidth on the paths. They do not reduce their load on the network when subjected to packet drops. This will result in aggressive capacity consumption by unresponsive protocols in competition with the behaved transport protocols such as TCP and SCTP.

Lack of fairness is the main problem of the above issue that TCP flows reduce their transmission rates in response to congestion, and UDP datagrams use the available bandwidth. This problem will be highlighted more particularly in the mobile network that a combination of UDP and TCP flows need to transfer on the line simultaneously and the volume of UDP connections are high.

1.1.3. Provision of Mobility

In mobile communications, links and data flow are involved in two major mobility models known as micro and macro mobility (intra-domain and inter-domain handover respectively). In micro or intra-domain mobility, handovers are within a subnet which means changes on mobile terminals' IP addresses are not needed. The major problem arises in a situation when a mobile node moves between two subnets, considering that by definition subnets have different network prefixes. In this case, resuming the connection is subject to releasing the old IP address, acquiring a new IP address from the new subnet, registering it with the home location register in the terminal's home network and finally informing the corresponding node to resume the connection on the new IP address. This procedure will cause termination of current flow and resuming the communication to the new address of mobile node. It also needs to resubmit all the packets that have not been acknowledged, and thus synchronize the packet transmission between the two IP addresses. The situation will deteriorate when there are several ongoing sessions at the same time. In that case, all the corresponding nodes would have to be notified of the new IP address and all of them have to synchronize the transmission.

In the worse case of the above scenario, a group of mobile nodes moves together. In group mobility scenarios such as mass public transportation in a train or coach, for some purposes it would be preferable for the system to be able to deal with co-located moving terminals as a group, and for a range of functions

pertaining to these terminals to be performed for the group as one. This would improve the efficiency, and likely the reliability, of radio resource control.

1.2. Contributions of this Thesis

Solutions that can be used to address the above cited challenges for moving network which are discussed and presented in this thesis are as follow:

- Soft and seamless vertical handover for moving networks
- Advance fairness and robustness in all IP mobile networks
- QoS provisioning of multi-link / multi-homed communications

Also they are summarised in this section.

1.2.1. Soft and seamless vertical handover for moving networks

Each layer of network protocol stack could be taking a particular role in the next generation of mobile networks in order to create advance mobility management. Different layers can have different responsibilities to develop a soft and seamless handover in intra and inter domain mobility. Suggesting which layer/layers are most suitable for mobility management is a challenging issue that depends on the system requirement, QoS parameters and the ability for changes in the network architecture that have been addressed in this thesis. Consequently, based on the focus of this thesis a suitable protocol for network mobility has been proposed.

By growing the generation of mobile nodes and networks in all IP scenarios the demands for high data rate transmission in high speed vehicle and public transport were increased. Recently the need for developing a new mobility management protocol has become an essential part of the telecoms research communities.

Network mobility introduces a new area of mobility scenario with the assumption that a group of mobile hosts moves together, performing similar tasks and they can form a single network unit. NEMO basic solution [2] uses Mobile IPv6 [6], which was originally designed for host mobility, with some additional tunnelling to manage the mobility for moving networks.

Efficient network mobility handover is essential to meet the QoS parameters. NEMO suffers from tunnelling overheads while it still inherits the well-known MIP issue which is long handover latency and results in high packet losses and severely reduces its end-to-end performance particularly in vertical handovers[2].

In this thesis a new mobility management protocol for a moving network based on Stream Control Transmission Protocol (SCTP) at the transport layer has been proposed. SCTP facilitated with multi-homing that has been used to handle the mobility issues within mobile network and developing nSCTP (NEMO-SCTP). The concept of nSCTP is "make before break", using more than one separated interfaces. This can be done in the overlap area of cells in a cellular network topology. While still one of the interfaces is communicating with the old domain, a new connection with the new domain will be established. In the later stage in a suitable time transmission will be switched to the new interface and the communication will be resumed.

Detailed structure and signalling for nSCTP is taken into consideration in this thesis and the performance of this newly developed protocol has been tested through analysis and simulation studies.

1.2.2. Advance fairness and robustness in all IP mobile networks

nSCTP uses a tunnelling method at transport layer in the wireless part of the network. This increases the QoS parameters by moderating the irresponsible protocol (e.g. UDP) that is discussed in section 1.1.2. These greedy protocols do not reduce their transmission rate when the communication is subjected to congestion and they will be taken over all or the greater portion of the available bandwidth in competition with the fairness conforming transport protocol (e.g. TCP). This problem has been addressed in nSCTP by introducing a transport layer tunnelling exactly at the bottleneck section of communication which is more vulnerable to congestion or packet loss. Therefore, the fairness of the system will be increased at the presence of nSCTP.

Retransmitting the packet when it is subjected to loss due to congestion or noise is the main source of inefficiency in any reliable data transmission. In a combined wired – wireless scenario, packet loss in the wireless part of the

network is commonly due to instability of the wireless media. A local retransmission of lost packet could greatly enhance the performance of the network if the systems overhead do not apply a huge amount of signalling and processing on the communication link. Developing this solution within nSCTP to activate a local retransmission between a mobile router's home-agent in the wired part of the communication with a mobile router which is used as a gateway of the mobile network is another contribution of this thesis. This solution introduces a new processing delay on the communication path but increases the performance of handling errors on the wireless hope(s) or portion of the system. Analysing the performance of the system and discovering the optimal threshold of lost packet in the wireless and wired part of network have been addressed.

1.2.3. QoS provisioning of multi-link / multi-homed communications

The growth of wireless and mobile communications has caused a wide selection of different wireless access technologies to be available in many places throughout the world. These technologies are often designed to fulfil particular purposes or to provide an alternative level of Quality of Service (QoS). In such a situation, if the users were able to dynamically switch between these technologies based on their requirements or available QoS, without breaking the connections, the user's satisfaction could be greatly enhanced. In order to apply dynamic switchover in a moving network scenario, probing signals have been added to the SCTP and nSCTP protocols in order to monitor the QoS parameters such as available bandwidth and end-to-end delay along with reconfiguration policies within the SCTP association. In such a case, probing signals periodically monitor the associated links and based on different predefined policies (aggressive, conservative and lagging) switch to the appropriate link. Enhancing the SCTP and nSCTP protocol to support the new signalling algorithms and switch over strategies is part of the contribution of this thesis. Implementing this structure in a simulation platform to study the performance of probing signals along with different policies has proven the usability of this enhancement.

1.3. Content of this thesis

After providing some overview to this thesis, the precise content is now introduced. The reasoning and justification behind each of the investigated/proposed technologies is discussed on a chapter-by-chapter basis.

1.3.1. Mobility Management Solutions (Chapter 2)

An important aspect of mobile network performance is mobility management. Through creating mobility management protocols, it is possible to handle handover in different layers of the OSI reference model and thus to infer any requirements that might be needed of the network to carry the traffic load adequately while providing an appropriate QoS to end-users.

To answer the question of which layer(s) is(are) more suitable for handling the mobility is challenging in the mobile network, especially in a heterogeneous infrastructure where moving networks or mobile nodes are involved in vertical and horizontal handovers. In addition, the specification of available wireless technologies in a heterogeneous environment and their impact on the mobility issues is another important part of mobility managements that should be addressed.

In this chapter, a hierarchical model of aspects of mobility management is presented and different proposals for mobility managements are considered. Network, transport and application layers mobility management solutions are taken into consideration. Group mobility management solutions which are the main focus of this thesis are presented.

1.3.2. Multi-homing and group mobility management challenges (Chapter 3)

In group mobility scenarios such as mass public transportation in a train or coach, for some purposes it would be preferable for the system to be able to deal with moving terminals as a group, and for a range of functions relating to these terminals to be performed for the group as one. For example, through enhanced algorithms for mobility control, the system would be able to infer that a large

number of terminals are about to handover to a new cell, if they are considered as a group the member of that group are not involved in handover issues. This would improve the efficiency, and likely the reliability, of mobility management.

For a single mobile node, there are different basic approaches for performing multi-homing that have been considered in detail in chapter 3 and a variety of challenges have been considered. Multi-homing is gaining more interest recently in mobile networks. A mobile network wishes to be multi-homed for the purposes of ubiquitous access, load sharing, reliability and aggregated bandwidth. There are different methods of multi-homing for NEMO that are discussed in this chapter. For the purpose of multi-homing in this thesis a single mobile router, a single home agent and a single mobile node prefix have been considered.

The proliferations of wireless technologies have given rise to the possibility of multiple accesses for a mobile multi-homed host. There are several reasons for multi-homed mobile networks that can refer to the aspects of fault resilience and redundancy, load balancing, service value and policy. There are different approaches to multi-homing in different layers of the OSI reference model. Multi-homing related works have been considered in this chapter and a comparison of benefits and drawbacks of each solution have been considered.

Also, in this chapter the challenges introduced by the use of network mobility, and different related works on group mobility managements are provided. This chapter provides a comparison between the solutions and introduces NEMO basic support protocol [2] which is the platform for the next chapters of this thesis.

1.3.3. nSCTP: Seamless Handover for Moving Networks (Chapter 4)

As has been mentioned previously and will be discussed more in detail in chapters 2 and 3, network layer solutions for mobility management cannot fulfil the requirements for mobility management that will be listed in chapter 2. SCTP has been proposed in RFC2960 [3] as an end-to-end reliable transport protocol operating on top of IPv4/IPv6 that provides network-level fault tolerance by supporting host mobility at either end of the connection. Applying this protocol

for a group mobility scenario will provide many limitations like software incompatibility and hardware limitations as a multi-interfaces node in mobile networks are not always achievable.

The scenarios investigated in this chapter contain the new tunnelling scheme that can be applied for moving network in NEMO basic protocol support. In this scenario SCTP-in-IP and IP-in-SCTP tunnels have been proposed and the algorithms for these tunnels have been proposed and illustrated in detail under two major modules named SCTP/IP encapsulator and SCTP/IP decapsulator. This tunnel has been used to develop a new protocol which uses the multi-homing feature of SCTP to handle the seamless handover over heterogeneous wireless networks.

Considering the challenges introduced by the use of multi-homing, particularly in mobile network communications scenarios, which could be beneficial for the nodes inside the mobile networks, is the concern of this chapter. nSCTP is proposed in this chapter based on SCTP/IP to facilitate multi-homing feature of SCTP for the mobile networks without involving the drawbacks of this protocol that have been mentioned before.

In the light of these observations, this chapter is concerned with dynamic switching between interfaces made available between the mobile router and the mobile router's home agent. The range of work performed looks at the practicality of multi-homing and its challenges, dynamic switching, signalling path and enhancement for Mobile Router and its home agent. Hence the conceived protocol is generally applicable to a range of mobile networks, requiring no changes in the Internet infrastructure, fully transparent to the end users and is also extremely computationally simple and efficient.

1.3.4. Performance analysis for end-to-end parameters in nSCTP and NEMO (Chapter 5)

More specifically to nSCTP protocol, there are a number of benefits for handling the micro and macro group mobility that can be named as reduction in handover delay and packet loss when the MR is moving. The main drawback of this newly proposed protocol is increasing the signalling overhead by adding another

reliable protocol into the middle of a given end-to-end connection that could reduce the performance of nSCTP compared to NEMO, which has been used as a guideline of this investigation. Moreover, SCTP/IP encapsulation which has been briefly described in section 1.3.3 and is further explained in chapter 4 can increase the outer tunnel overhead in NEMO basic protocol [2], which results in reducing the overhead.

In this chapter, for considering the mentioned trade off between overhead and signalling, an analytical model for both NEMO and nSCTP have been developed. Detailed investigations for NEMO and nSCTP in terms of handover delay, packet loss and throughput are provided. For a firm comparison of analytical results in NEMO and nSCTP numerical examples are provided.

1.3.5. Simulation studies of the performance of SCTP and nSCTP (Chapter 6)

Challenges and possible solutions introduced by the use of reliable transport layer protocols taken into consideration through a simulation study in the wired and wireless scenario. Network simulator ver.2 (NS-2) has been introduced to use as a platform for the simulation studied in this thesis. Firstly, for proof of concept a simulator is established to use SCTP as a reliable transport protocol in a wired-cum-wireless scenario. A firm comparison between different versions of TCP and SCTP showed that SCTP can have better or at least equivalent performance compared to other reliable protocols. The concept of multi-homing and using that feature for handling the mobility is the second set of simulation and finally the last part of simulation, which is still an ongoing part of this chapter, is allocated to the main concentration of this thesis which is developing of nSCTP.

1.3.6. QoS provisioning for SCTP (Chapter 7)

As has been discussed previously in this Introduction, traditional SCTP [3] uses multi-homing as an alternative path to the primary link means that an unsuccessfully delivered packet is retransmitted through the secondary path. Also, a certain number of consecutive packet losses will cause swapping of the

primary paths with the secondary. This feature along with ADD-IP extension of SCTP [7] formed some of the transport layer handover managements such as mSCTP [8] and nSCTP[9]. This scheme of failover however provides a soft and seamless handover but the number of packet losses during the handover period are still high and on the other hand, the association between multi-homed entities is only aware of the existence of the alternative paths and has no information about the quality of each path.

In spite of all the benefits and advantages of SCTP, the failover mechanism of this protocol does not adapt to application requirements or network conditions. In other words, an association will insist on staying with a defined primary link until it is disconnected completely or a certain number of consecutive time-outs are experienced, while some higher quality links may be available.

In this chapter a novel solution to improve the SCTP's failover mechanism, named as "switchover" in this thesis, is presented. The efficiency of this protocol has been tested by implementing a simulation model on NS-2 platform. The result depicted that dynamic handover can significantly improve the efficiency of SCTP particularly in the area with different choice of wireless access networks and movement that frequently can affect the quality of received signals.

Chapter 2. Wireless Communication and Mobility Management

2.1. Introduction

The Internet has been designed for static wired connections and originally was a combination of several nodes and networks. Demand for "anywhere, anytime" communications has been increasing recently and consequently wireless mobile nodes have been introduced. These nodes need to keep their connectivity while they are moving. Mobility management is an intelligent function of wireless mobile nodes that keeps track of movement and communications. When a mobile device is roaming through one or more service areas, mobility management mechanisms are required to keep the ongoing sessions alive. Broadly speaking, mobility management can be classified into location management and handover management.

1. Location management: This function is used for discovering the mobile node's current point of attachment. Location management is responsible for location update and data delivery. Location update in definition is keeping track of the mobile terminal by sending notification periodically. Current position of a mobile node should be kept in a database and is used to deliver data or a call to the location area of the MN.
2. Handover management: It is responsible for enabling users to keep their connections alive as they move and change their point of connection to the network.

As the Internet is structured in a-five layer architecture; physical, data link, network, transport and application layers, there are many proposals to manage mobility in these layers. The natural question is which layer is preferable for mobility? A study done by Eddy [10] has compared the use of three different

layers for mobility. The work shows the common network layer solution, Mobile IP, has several weaknesses and limitation with regard to its effectiveness. The authors believed most of this problem can be tackled by a higher transport or session layer approach and suggested a transport layer solution as the strongest candidate among various levels. Ratola [11] introduces and compares three implementing mobility protocols, each from a different layer. The purpose of the comparison is to determine which layer - three, three and a half, or four - would be best suited for mobility. The chosen protocols are Mobile IPv6 (MIPv6), Host Identity Protocol (HIP), and Stream Control Transmission Protocol (SCTP) respectively. Ratola believes a new layer 3.5 is necessary because using lower layers do not have such a great impact and also a new transport layer protocol causes incompatibility in implemented software. In another study done by Atiquzzaman et al. [12] different transport layer solution for mobility management have been compared and they believe that a complete mobility scheme, which supports IP diversity, soft handoff, transparency to applications with no changes in the network infrastructure, is achievable in transport layer solutions.

A mobility management solution's efficiency can be evaluated based on the following terms[12]:

1. Packet loss during handover and handover latency: they are two crucial parameters for mobility management protocol to avoid any service disruption or connectivity.
2. Seamless handover: is the main goal for system with uninterrupted mobility.
3. Compatibility with IP addressing routing protocols: The Internet is following a hierarchical IP addressing and routing structure with which mobility solutions should be adapted.
4. Application layer transparency: Mobility management mechanisms should not affect the upper layer protocols.
5. Security: Mobility management protocols ideally should not inject new security issues or vulnerabilities into the network.

6. Change in Internet infrastructure: The mobility solutions should avoid making changes in either the infrastructure of the Internet or the network layers and standards.

Performing individual handovers for a group of users which are roaming together can cause huge signalling overhead. Network mobility support is a solution to overcome this problem. In this type of scenario, a whole network is viewed as a single unit, which changes its point of attachment to the Internet and thus its reachability in the Internet topology. In such a network one or more mobile routers connect the local fixed and visiting mobile nodes inside the network, to the Internet. The Local Fixed Nodes (LFNs) in a moving network are unable to change their point of attachment to the MR's network. These nodes are mobility unaware nodes, meaning that they do not have any mobility software running on them. Also a Visiting Mobile Node (VMN) is a node downstream of the MR which is capable of joining/leaving the MR's network when necessary. VMNs are mobility aware nodes, meaning that they must have mobility software such as MIPv6 installed and running.

NEtwork MObility (NEMO) [2] is a protocol extension to Mobile IPv6 (MIPv6) [6] to provide support for network mobility. It also allows every node in the Mobile Network to be reachable while moving around. The MR(s), which connects the network to the Internet, runs the NEMO Basic Support Protocol Solution with its Home Agent. The protocol is designed so that network mobility is transparent to the nodes inside the Mobile Network.

In this chapter, we will explain briefly Mobile IP functionalities and its abilities and follows by a discussion about group mobility management or train scenario.

Key terminology definitions in this chapter:

- Mobility: is defined as the ability to maintain a continuity of the service regardless of terminal mobility, personal mobility or service mobility.
- Vertical handover: is a type of link that would provide the necessary bridging over and through different networks in order to establish an efficient inter-work between networks entities.
- Coupling between networks: is the level of inter-working which distinct between various proposed inter-working architecture models.

- Technology intelligence: a device, node or even a network is said to be intelligent when it takes care of the most routing/signalling/addressing and handover operations in an efficient and reliable manner.
- Soft Handover: During a soft handover there are two simultaneous active links, therefore, we will not have any packet lost. As the bandwidth and throughput may be totally different between two contributing subnet works, delay and jitter can be larger than required.
- Hard Handover: With a hard handover, it is possible that two links co-exist during a period of time, but only one of them is active at a certain point in time. Therefore, in a hard handover there is the possibility of a temporary break in the communication.

2.2. Heterogeneous environment in mobile communications

There are three different generations as far as mobile communication is concerned. The first generation, 1G, was established in the mid 1980s. 1G is a semi analogue mobile network because it uses an analogue radio path with digital switching. The most popular 1G mobile networks are Nordic Mobile Telephone Systems (NMT) and American Mobile Phone Systems (AMPS) [13, 14]. These networks provide only basic services (such as speech and speech-related) for users. 1G networks have national specifications. Therefore, 1G networks are incompatible with each other.

The 2G was established in early 1990s. The emphasis in this generation was the compatibility and the international transparency. From the user's point of view, 2G networks offered a more attractive "packet" to buy; in addition to traditional speech service these networks were able to provide some data services and more sophisticated supplementary services. Due to the regional nature of standardization, the concept of globalization did not succeed completely. The most popular 2G systems in the market are Global Systems for Mobile Communication (GSM) and IS-95. The 2G networks had some problems such as: slow data rate, long connection setup time and expensive services. The reason for

this is that these networks are mainly designed to deal with circuit switch voice and each channel is dedicated to only one user.

The General Packet Radio Service (GPRS) has been developed to address these issues by providing the packet switch bearer service. GPRS applies packet radio principles to efficiently transfer data between GSM mobile stations and external packet data network. GPRS provides connection set up time of 1 second and data rates up to several tens of Kbits/s.[13] (The theoretical maximum GPRS data rate is 171.2 Kbps per channel.)

The 3G can be considered as the next step beyond GPRS. The third generation is expected to complete the globalization process of mobile communication. Universal Mobile Telecommunication Systems (UMTS) and CDMA-2000 are the two main 3G networking standards. The emphasis of this thesis is on UMTS which has been approved as the standard for the UK and other European countries by the European Telecommunications Standards Institute (ETSI) [15]. UMTS is the third generation of cellular networks, offers advanced features such as: high data rate (144 Kbps for satellite and rural outdoor, 384Kbps for urban outdoor, 2Mbps for indoor and low range outdoor) and improved QoS services to users. UMTS also provides better frequency efficiency and lower transport costs using ATM network for both voice and data services.

UMTS provided a platform to combine different services such as: speech and data with the Internet. From a commercial point of view, UMTS creates a global market for mobile multimedia with vast opportunities for new revenues, such as:

- Providing a wide variety of new multimedia and entertainment services
- Offering personalized news and information
- Providing a targeted advertising channel and stimulating income from Web referrals
- Deploying services that facilitate transactions

In Figure 2-1 the functionality and time generation progress is summarized.

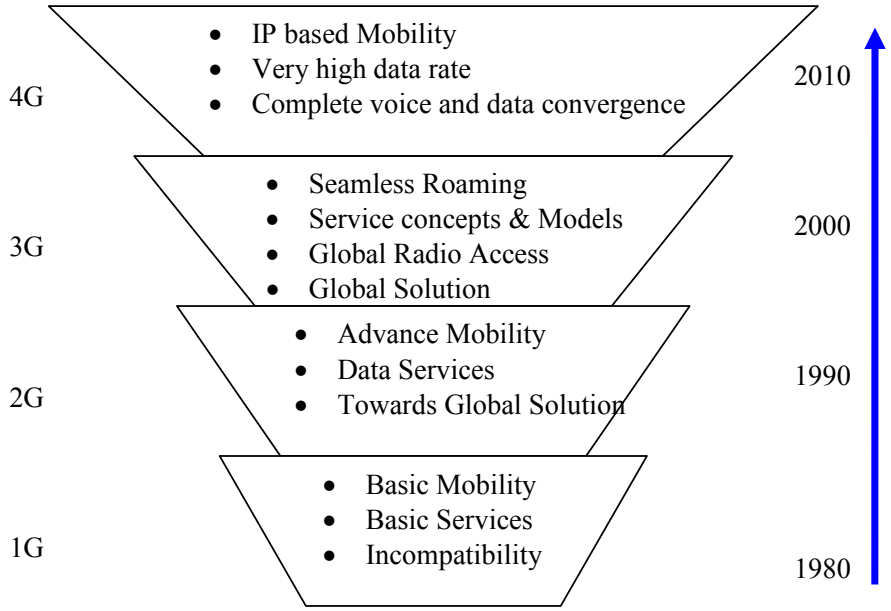

Figure 2-1: Summary of the functionality of different generations of mobile networks

2.2.1. UMTS

2.2.1.1. Architecture

As illustrated in Figure 2-2, a UMTS network consists of three domains: Core Network (CN), UMTS Terrestrial Radio Access Network (UTRAN) and User Equipment (UE) [14].

- Core Network (CN): The CN includes physical entities to provide network features and telecommunication services. These support management of user-location information, control of network features and services, and the transfer mechanism for signalling. In the CN, the traffic is either circuit-switched or packet-switched in nature. Therefore, the CN is divided into two sub-domains: Circuit Switched Domain (CS) and Packet Switched Domain (PS).

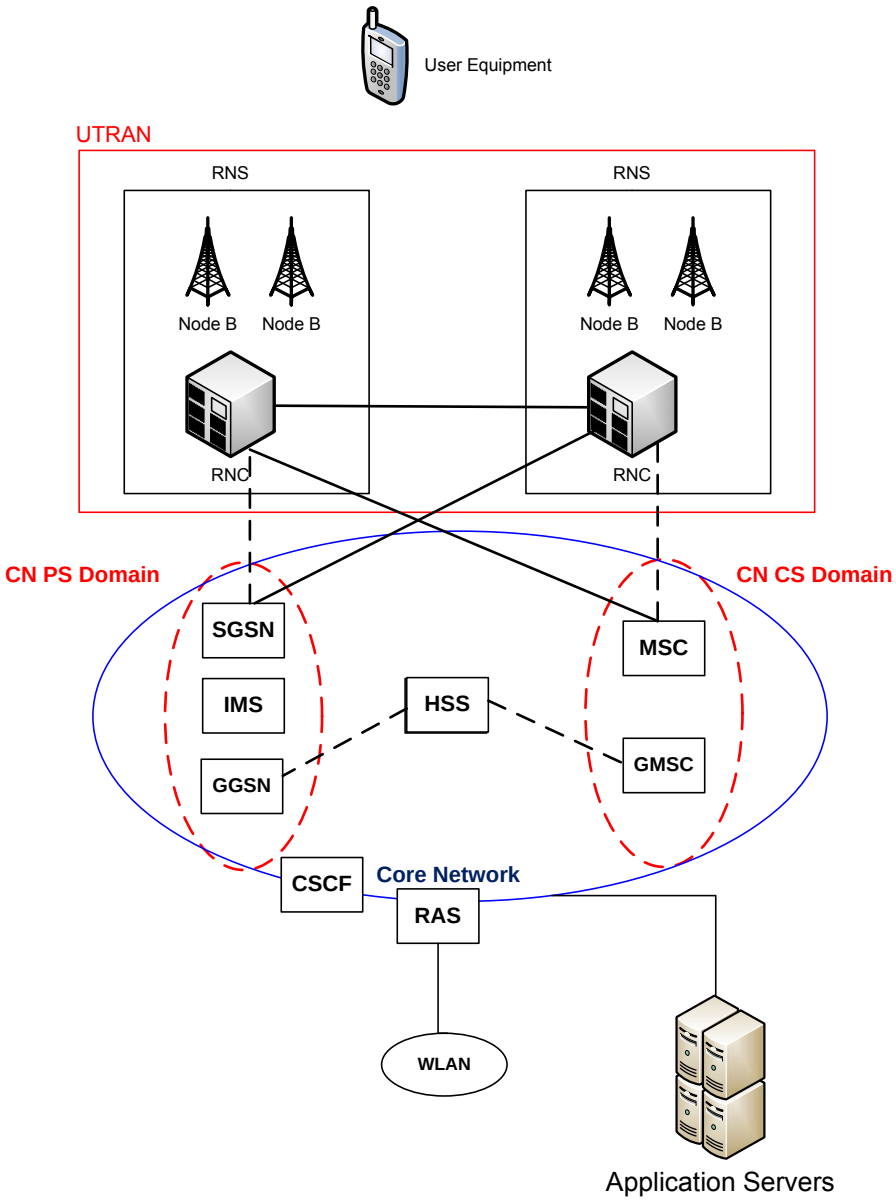

Figure 2-2: UMTS architecture

- UMTS Terrestrial Radio Access Network (UTRAN): UTRAN consists of RNCs and Node-Bs, which are shown in section Figure 2-2.
- User Equipment (UE): UE is used to access UMTS services such as speech, SMS, emergency calls, etc. This domain includes a variety of equipment with different levels of functionality, e.g. the user equipment might have a removable smart card. This domain is divided into two parts: Mobile Equipment (ME) Domain and User Services Identify Module Domain (USIM).

2.2.1.2. UMTS Components

The components of UMTS architecture are as follows:

- GGSN (Gateway GPRS Support Node): Provides access to the services area over the Internet
- SGSN (Serving GPRS Support Node): Provides the functions of network access node and mobility management
- IMS (IP Multimedia System): Responsible for delivering internet services over GPRS. It supports other networks and provides an open standards-based network that delivers integrated multimedia services.
- MSC (Mobile Switching Centre): Contains connection management functionality. The MSC server is also responsible for mobile management and contains the VLR (Visitor Location Register).
- HSS (Home Subscriber Server): Is an evolution of the Home Location Register. HSS provides storage for relevant information for both GSM and UMTS subscribers. HSS has two parts: User Profiles and User Locations.
- GMSC (Gateway Mobile Switching Centre): works as a gateway between PLMN (Public Land Mobile Network) and PSTN (Public Switched Telephone Network) in order to provide the necessary signalling and convert traffic formats between two networks. For mobile terminated calls, it interacts with the HSS to obtain routing information.
- RNS (Radio Network Subsystem): Contains one RNC and is responsible for the resources and Transmission/Receiving in a set of cells.
- RNC (Radio Network Controller): Enables autonomous Radio Resource Management (RRM) by UTRAN and is responsible for controlling the use and integrity of the radio resources. RNC also assists in the soft handover of UEs when a UE moves from one cell to another.
- Node B: Is a physical unit of radio transmission/reception within a cell. It can support both TDD and FDD modes. Node-B is responsible for Forward Error Correction (FEC), rate adaptation, W-CDMA spreading/dispreading and QPSK modulation on the air interface.

2.2.2. WLAN

Wireless LAN technology has evolved to extend LANs, which was emerged during 1970s to enable sharing of expensive resources such as printers and to manage the wiring problem caused by increasing number of terminals in offices. By the early 1980s, three standards for LAN were developed: Ethernet (IEEE 802.3), Token Bus (IEEE 802.4) and Token Ring (IEEE 802.5); they each specified distinct physical (PHY) and medium access channel (MAC) layers and different topologies for networking. Currently, LANs are mostly based on switched Ethernet technology that consists of an interconnection of hosts and routers. The 802.11 [16] industry standard and its various revisions are a particular form of Wireless LAN. 802.11 WLAN is commonly referred to as "Wi-Fi" (Wireless Fidelity). The IEEE802.11 Working Group was formed in 1990 to define standard physical (PHY) and medium-access control (MAC) layers for WLANs in the publicly available ISM (Industrial, Scientific and Medical) bands. The original goal was to have data rates of 2Mbps, falling back to 1 Mbps in the presence of interference or if the signal became too weak.

Since then, several task groups (designated by letters) have been created to extend the IEEE 802.11 standard. Task groups 802.11b [17] and 802.11a [17] have completed their work by providing two relevant extensions to the original standard. The 802.11b task group produced a standard for WLAN operations in the 2.4 GHz band, with data rates up to 11Mbps. This standard, published in 1999, has been very successful in its deployment in public places. The 802.11a task group created a standard for WLAN operations in the 5GHz band, with data rates up to 54Mbps. Among the other task groups, it is worth mentioning task group 802.11e (which propose algorithms to enhance the MAC with QoS features to support voice and video over 802.11 networks) and task group 802.11g (which is working to develop a 54Mbps data rate extension to 802.11b at 2.4 GHz).

Wireless LANs can provide almost all the functionality and high data-transmission rates offered by wired LANs, but without the physical constraints of the wire itself. Wireless LAN configurations have wide variety of applications from temporary independent connections between two computers to managed data communication networks that interconnect to other data networks (such as the

Internet). Data rates for WLAN systems typically vary from 1 Mbps to more than 100 Mbps.

Wireless LAN systems may be used to provide service to visiting users in specific areas (called “hot spots”). Hot spots are geographic regions or service access points that have a higher amount of usage than average. Examples of hot spots include wireless LAN (WLAN) access points in a trains, buses, railway stations and coffee shops.

2.2.2.1. WLAN Components

- End User Access Devices (Stations): End user access devices are called stations (STA) in a WLAN system. End user stations are transmitter and receiver that convert radio signals into digital signals that can be routed to and from communication devices.
- Access Points (APs): An access point (AP) is a radio access transceiver (combined transmitter and receiver) that is used to connect wireless data devices (stations) to a Local Area Network (LAN) system. Access points convert and control the sending of data packets and can connect one or many wireless devices to a wired LAN[16]. Access points can perform one or many types of data transfer functions including bridging (linking networks), retransmitting (repeating), distributing (hubs), directing packets (switching or routing) or to adapt formats for other types of networks (gateways).
- Gateway: Gateways are communications devices or assemblies that transform data that is received from one network into a format that can be used by a different network. Wireless gateways are access points that can assign temporary IP addresses (DHCP) to nodes and have the ability to share a single public IP addresses with several private IP addresses.

2.2.3. Wireless Metropolitan Area Network (WMAN)

Wireless metropolitan area network (WMAN) are wireless networks that provide data communication access throughout an urban or city geographic area. There are thousands of WMANs that are in use throughout the world and the common

applications include interconnecting law-enforcement, public utility, or public safety communication services.

With the introduction of Broadband Wireless Access (BWA) technology, WMANs can be used to provide broadband access to public users in an urban area. This allows WMAN systems to compete with other technologies such as Digital Subscribe Line (DSL) and cable modems.

To develop a cost effective, high-speed data transmission WMAN system, the IEEE created the 802.16 [18]. The 802.16 systems is a line of sight system that operates in the 10 to 66 GHz of radio spectrum. WiMAX (World Interoperability for Microwave Access), based on the IEEE 802.16 standard, is aimed to provide wireless data over long distances, in a variety of different ways, from point to point links to full mobile cellular type access.

2.3. OSI reference model and mobility management

The OSI reference model breaks the communication into seven layers. Each layer has a well-defined scope of its functions clearly. When it comes to mobility management, there are techniques that can be used at each layer. This section gives a brief overview of these techniques.

- Physical Layer: this layer transmits the bit stream over an interface or media between sender and receiver. The air interface in wireless communication is responsible for carrying radio signals and finally the data from sender to receiver antennas.
- Data Link Layer: is responsible for specifications of the logical connection across a physical link. This layer also manages the Pico-mobility. The Media Access Control (MAC) and the Logical Link Control (LLC) are the data link sub layers. Permission to transmit data, frame synchronization, flow control and error checking are the main defined object for this layer. The wireless networks include cellular networks, Wireless Local Area Networks (802.11), WiMAX Networks, and home area networks (Bluetooth) are some example of wireless protocols in this layer.

- Network Layer: this layer provides switching and routing technologies. Addressing, internetworking, error handling, congestion control are the other function of third layer of OSI reference model. Network layer in mobile networks besides the addressing and care of MN addressing is responsible for location and handover management. Mobile IP (MIP) [1] is one of the most important protocols for macro mobility management and Hierarchical Mobile IP (HMIP)[19] is a sample for Micro-mobility roaming.
- Transport Layer: this layer is responsible for transparent transfer of data between two end systems. This layer provides error recovery and flow control and the key differences with network layer is that transport layer is end-to-end while network layer is a point-to-point chain between routers. This layer also can provide functionality for multi-homing and handover management in mobile networks. mSCTP[20] is an example of a handover management protocol in this layer that uses the multi-homing feature of SCTP to handle micro and macro mobility. Mobile SCTP (mSCTP) [21] is the new extension of SCTP that uses the multi-homing feature of SCTP to manage handover in wireless networks. The mSCTP needs to use a location management protocol like Mobile IP (MIP) [1], Session Initiation Protocol (SIP) [22] or any other location management protocol to complete the mobility management process, the details of this is explained in the next chapter and further information is available in [23 2006].
- Session, Presentation and Application Layers: these layers which mostly recognised as application layer support applications and end users' processes. Authentication, Authorization and Accounting (AAA) that are part of security in computer networks is part of the tasks in these layers. In mobile communication, this layer can perform a role in handover management and location management. Session Initiation Protocol (SIP)[22] is an example of location management that operates in this layer.

There are many proposals to manage mobility in different layers of protocol stack that some of them are addressed in the following sections.

2.4. Application based terminal mobility

Session Initiation Protocol (SIP) is the main mobility management protocol in application layer, specified in IETF RFC–3261 [22]. SIP can establish, modify and terminate multimedia sessions. The main function of SIP is to establish real-time calls and conferences over internet-protocol networks. Each session may include different types of data, such as audio and video, although currently most SIP extensions address audio communication. [24]

SIP defines a number of components, namely user agents (application that initiates the SIP request), redirect servers (gives the client information about the next hops the message should take), proxy servers (receives SIP messages from a client or another proxy server and forwards the messages to the next SIP server in the network) and registrars (deals with current-location of user agent registration). SIP inherently supports personal mobility and can be extended to support service and terminal mobility. Terminal mobility allows a device to move between IP sub-nets, while continuing to be reachable for incoming requests and maintaining sessions across subnet changes. Mobility of hosts in heterogeneous networks is managed by using the terminal mobility support of SIP.

Terminal mobility requires SIP to establish a connection either during the start of a new session, when the terminal or MN has already moved to a different location, or in the middle of a session. The former situation is referred to as pre-call mobility, the latter as mid-call or in-session mobility. For pre-call mobility, the MN re-registers its new IP address with the Registrar server by sending a REGISTER message, while for mid-call mobility the terminal needs to intimate the Correspondent Node (CN) or the host communicating with the MN by sending a re-INVITE message about the terminal's new IP address and updated session parameters. The MN also needs to register with the redirect server in the home network for future calls. Figure 2-3 shows the messages exchanged for setting up a session between a mobile node and a correspondent node and continuing it after changing the access network.

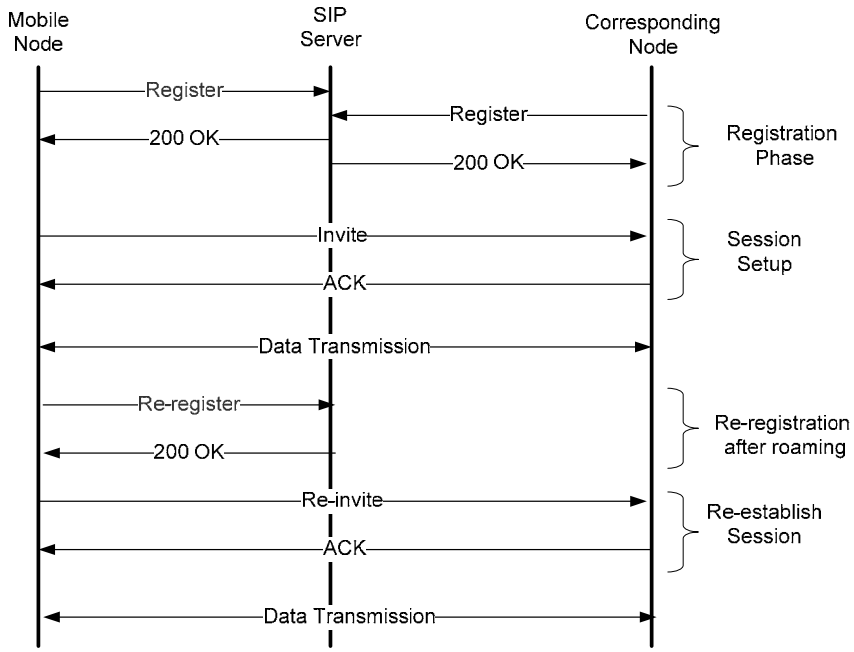

Figure 2-3: SIP signalling

SIP suffers from some drawbacks[25]. Firstly, the SIP session must be setup completely while the mobile terminal is in the overlap area of the cells to avoid connection disruption. Secondly, mobile node should acquire the IP address via DHCP that can increase the handover delay.

2.5. Transport layer based mobility

The single point of failure often is the main weakness of most end-to-end connections. This failure can happen in the wired or in the wireless part of the connection. In the wired part of the network, the failure may happen because of the medium or router problem that routing protocols can tackle by using different rerouting techniques. In the wireless part, the link failure can occur because of random errors in the medium, low bandwidth and mobility. It is reasonable to say that the link failure is more likely in the wireless than in the wired part of the network. Link failure has direct effect on higher layers, as transport-layer connections rely on the network connectivity and applications rely on the transport-layer connections. This is the main drive behind this work to develop a

novel transport layer solution for dealing with random link failures in mobile networks.

Multi-homing is a concept that has been gaining more interest in the research communities [12]. Multi-homing addresses the problem of single point of failure by using the alternative connections. This feature provides both endpoints with multiple communication paths and thus the ability to failover (switch) to an alternative path when the link failure occurs. The simultaneous connectivity can be realised using multiple ISPs or multiple wireless access technologies, such as cellular networks (e.g. GPRS, UMTS) and wireless LANs and MANs (e.g. 802.11, WiMAX).

The current transport protocols, TCP and UDP, do not support multi-homing. TCP allows binding to only one network address at each connection ends. This is the main reason why a new transport-layer protocol, Stream Control Transmission Protocol (SCTP) [3], is being investigated in this research. SCTP is a general purpose transport layer protocol providing reliable ordered delivery of data (like TCP) and also unreliable data message (like UDP). SCTP also featured with multi-homing and multi-streaming capabilities.

2.5.1. SCTP

Stream Control Transmission Protocol (SCTP) [3] is a general purpose transmission protocol for IP network data transmission. SCTP provides both reliable End-to-End data transmission, as TCP does, and unreliable data transmission, as UDP does. SCTP also supports partial reliable data transfer [26], which can be used in some applications and can carry reliable content - like text pages, billing and security information, setup signalling - as well as unreliable content e.g. multimedia packets or voice. SCTP provides message-oriented data transmission service. Each SCTP packet consists of a header and one or more data chunks and each chunk has also a header, which identifies its length, type, and any special flags the type needs. One of the features of SCTP is the flexibility of putting different chunk types into a single data packet. The only restriction, which imposes on the packet size, is that it cannot exceed the destination path's maximum transmission unit (MTU) size.

To appreciate the functionalities of SCTP, a comparison between SCTP, TCP and UDP is presented in Table 2-1.

Protocol Feature	SCTP	TCP	UDP
Reliable data transfer	Yes	Yes	No
Partial reliable data transfer	Yes	No	No
Connection oriented delivery	Yes	Yes	No
Congestion control and avoidance	Yes	Yes	No
Path MTU discovery and message fragmentation	Yes	Yes	No
Message bundling	Yes	Yes	No
Multi-homing	Yes	No	No
Multi-streaming	Yes	No	No
Ordered data deliver	Yes	Yes	No
Unordered data delivery	Yes	No	Yes
Path reachability check	Yes	No	No

Table 2-1: A summary of SCTP, TCP and UDP functionalities[27]

An SCTP connection, called association, includes two major new capabilities, multi-homing and multi-streaming.

2.5.1.1. Multi-homing

A host is called multi-homed if it is reachable or accessible through multiple IP addresses. This feature of SCTP, multi-homing, allows for binding of one transport-layer association to multiple IP addresses, which makes an SCTP sender capable of sending data to a multi-homed receiver through different destination addresses as illustrated in Figure 2-4. Therefore, if one of the IP addresses becomes unreachable, which could happen due to link failure as MN is too far from an access point, failing in ISP or failing in host's interface, the destination host can still receive data through an alternative interface.

The multi-homing feature of the SCTP allows binding of one transport layer association to multiple IP addresses at each end of the association. SCTP has a

built-in failure detection and recovery system, known as failover, which allows associations to dynamically send traffic to an alternate peer IP address when needed. SCTP's failover mechanism is static and does not adapt to application requirements or network conditions.

As a TCP connection uses a single IP address at each end host, the possible connections between host A and B, in Figure 2-4, are (A1,B1), (A1,B2), (A2,B1) or (A2,B2). SCTP connection allows association between all available IP addresses at each end point. Hence, an SCTP association between host A and B could consist of two sets of IP addresses: {(A1, A2), (B1, B2)}.

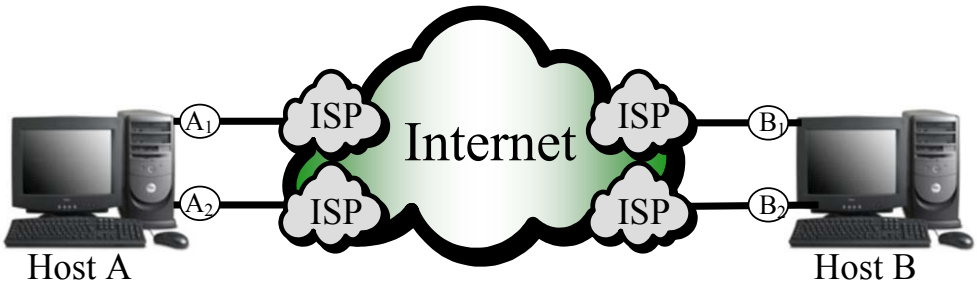

Figure 2-4: Multi-homing Scenario

This feature of SCTP is currently used for redundancy or fault tolerance. If one destination address becomes unreachable, the destination can still send and receive via other interfaces bound to the association. When the peer is multi-homed, an SCTP endpoint will normally be required to select one of the peer's destination addresses as the primary destination address. All other destination addresses or associations of the peer become alternate or backup addresses. The endpoints periodically check the availability and reachability of the links. In SCTP signalling, HEARTBEAT chunks are responsible for keeping the reachability status up-to-date [3].

In the case of error detection or packet loss, the end point re-transmits packets to an alternate address. Continued failure to reach the primary address ultimately results in failure detection, at which time the end point transmits all chunks to an alternate destination until the primary destination becomes reachable again.

2.5.1.2.Multi-streaming

Another important feature of SCTP is multi-streaming. In a TCP connection, all bytes received must be processed in the same order they were sent. For instance, if a segment is transmitted first, it must safely arrive at the destination before a second message can be processed even if the second segment arrives earlier. SCTP has the ability to process multiple segments (in any order of arrival) by sending segments in different streams. Therefore, SCTP distinguishes different streams of messages within one SCTP association.

Figure 2-5 shows a multi-streamed association between hosts A and B. During this example, host A requested three streams to host B (numbered 0 to 2), and host B requested only one stream to host A (numbered 0).

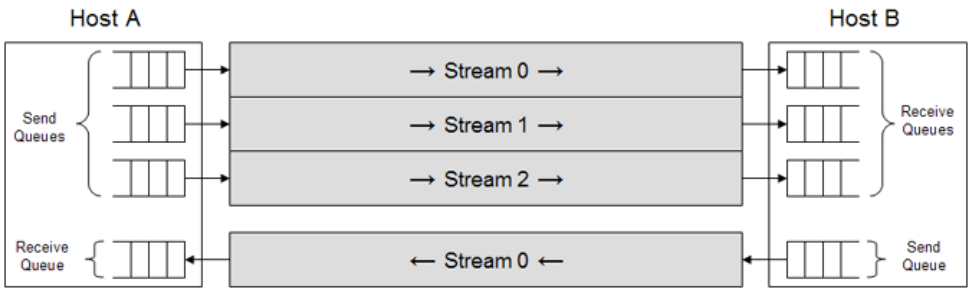

Figure 2-5: Multi-streaming Scenario

The multi-streaming allows independent delivery among data stream. Application data can be portioned into multiple streams. These portions or data chunks will be formed inside an SCTP packet and each packet can contain multiple data chunks from different applications. Chunks header contains Transmission Sequence Number (TSN), Stream ID and Stream Sequence Number (SSN) that can provide independent delivery of each stream to the application.

Figure 2-6 depicted the functionality of multi-streaming and multi-homing in an SCTP association. Multi-homing allows binding more than one IP address at each end and in the SCTP association this let the communication switch between this IP addresses. The links that is carry the transmission called “primary path” and the other link as “secondary path” which is an alternative path for packet

retransmission or failover purposes. Also, the functionality of multi-streaming allows different applications to handle via separated streams. This will solve the Head-of-Line (HoL) Blocking drawback of TCP that uses only one stream per communication link. Therefore in SCTP, if data on Stream 1 (S1) is lost, only Stream 1 is blocked at the receiver while waiting for re-transmission and other streams can still carry on the transmission without and disruption on their delivery.

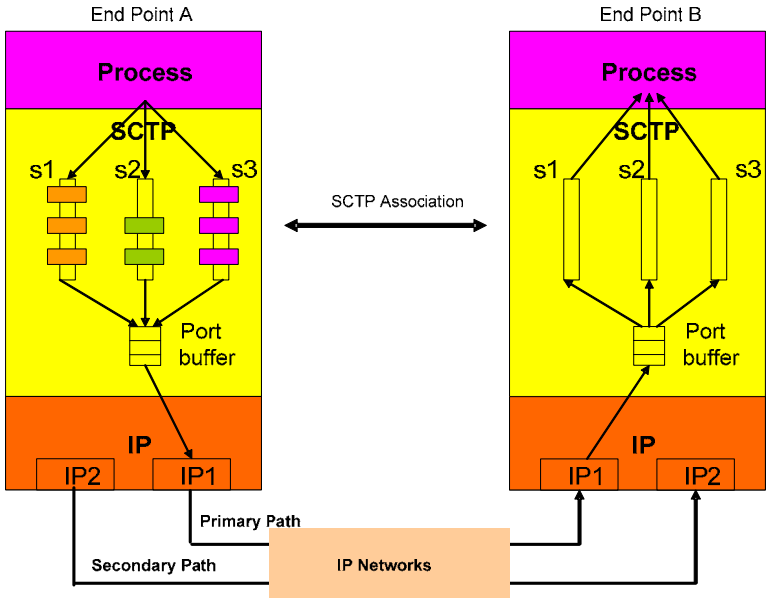

Figure 2-6: SCTP association with both multi-streaming/multi-homing features (End point A is a Sender and B is a receiver)

2.5.2. Mobile SCTP (mSCTP)

With the help of the dynamic address reconfiguration, the SCTP with the ADDIP extension (called mSCTP[8, 20]) would provide soft handover for the mobile terminals without any additional support of routers/agents in the networks. The ADDIP extension enables the SCTP to add, delete and change the IP addresses during active SCTP association. In this scheme SCTP with ADDIP takes care of handover and provides a soft and seamless roaming and a location management protocol like MIP or SIP is used for keep tracking of the MN movements.

Dynamic Address Reconfiguration (DAR) is an extended message to send Add-IP, Delete-IP and set Primary IP Parameters. In order to deliver these DAR

parameters, two additional chunks, Address Configuration Change Chunk (ASCONF) and Address Configuration Acknowledgment (ASCONF-ACK) are defined [7].

Figure 2-7 shows the ASCONF chunk format involved in DAR [7]. The Type field is filled with the value, 0xC1, to identify ASCONF chunk and the Flag field sets to 0 as it is not used in this chunk. The Chunk length field denotes the length of the chunk and serial number is used in order to distinguish a particular ASCONF chunk from other chunks. Address parameter is set to a sender address. ASCONF parameter fields contain add-IP, delete-IP, and set-primary-IP parameters.

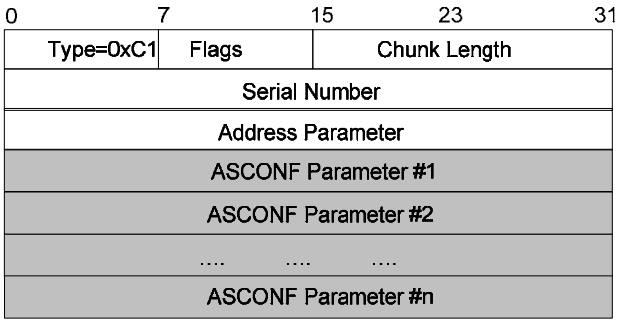

Figure 2-7: ASCONF Chunk Format

ASCONF parameters are formed in the shown structure in Figure 2-8. Type field gets the value of 0x001, 0x002, 0x004 for add-IP, delete-IP, and set-primary-IP parameters respectively. Length is the size of parameter, which depends on the address parameter length. The address parameter length as described in subsection 3.3.2.1 of RFC2960 is 8 bytes for IPv4 and 20 Bytes for IPv6. ASCONF-request correlation ID is used for a sender of the ASCONF chunk to distinguish the particular chunk from other chunks.

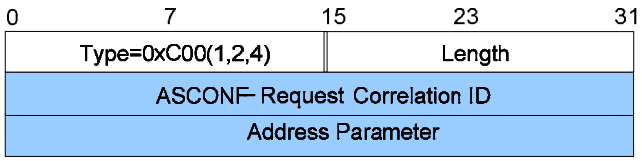

Figure 2-8: ASCONF Parameter format for Add-IP, Delete-IP and set primary-IP

Figure 2-9 shows the functionality of mSCTP in a micro and macro mobility scenarios. Mobility between cells 1 and 2 or cells 3 and 4 represents a micro mobility scenario that movements are within the domains. The movement from cells 2 to 3 that the domain has to be changed is a macro mobility scenario. The new location of the MN must be registered with MN Home agent. mSCTP can work in both scenarios by establishing a new connection with the new domain/cell on the free interface at the time the MN enters into the overlap area. At the suitable time when the second interface finished acquiring the IP address and registered it with MN's Home agent SCTP association between CN and MN switches over to the second interface. And finally when the MN leaves the overlap areas the old connection will be deleted form the SCTP association.

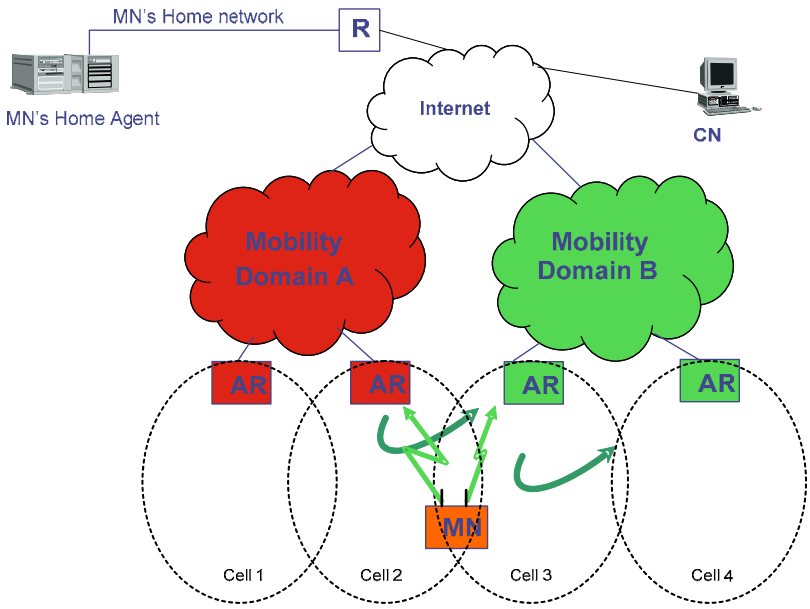

Figure 2-9: Micro and macro mobility in multi-homed scenario with mSCTP

The connection, handover procedure and exchange messages can be summarised as follow:

- Initiation of the session by a mobile client obtaining an IP address for a new location and sending ASCONF with Add-IP carrying the new IP

- Adding the new IP address to the SCTP association and sending ASCONF-ACK
- Changing the primary IP address, by sending ASCONF with Set Primary, rules for changing the primary IP address and the suitable time for the switch to a new address is a challenging issue of the mSCTP.
- Sending ASCONF-ACK and change the primary IP address
- Removing the old IP address from the SCTP association by sending ASCONF with Delete IP carrying the old IP
- Deleting the IP form the SCTP association and send ASCONF-ACK

2.6. Network layer based mobility

Mobile IP [28] is an extension to IP proposed by the Internet Engineering Task Force (IETF), which was designed to address IP addressing for mobile users. Mobile IP has been proposed as a solution for mobility support and provides users with the freedom to roam beyond their home subnet while consistently maintaining their home IP address.

Generally, mobile IP is most useful in the environments where a wireless technology is being utilized. This includes cellular environments as well as wireless LAN situations that may require roaming. Each mobile node is always identified by its home address, no matter where its current point of attachment to the Internet is, allowing for transparent mobility with respect to the network and all other nodes. Home address is the address that is allocated to the mobile node by its home agent and remaining unchanged while it is moving in different coverage areas. In MIP, the only devices that need to be aware of the movement of this node are the mobile node and a router serving the user's home subnet.

Mobile IP has three components as follows:

- Mobile Node (MN): is user equipment like Mobile phone, PDA or laptop.
- Home Agent (HA): is a router on the home network operating as the anchor point for communication for MN.

- Foreign Agent (FA): is a specialised router on the foreign network that MN is currently visiting and operates as a point of attachment for the MN to that foreign network. FA delivers the packets destined to MN from HA.

MIP is a network layer based solution for mobility management. It can provide a single approach solution for both addressing and handover managements for a mobile node. In MIP a Mobile Node (MN) should use two IP addresses: a permanent address or home address, assigned to the host and acting as its end point identifier; and the care of address (CoA), providing the host's fixed address. In MIP, the mobility agents known as Home Agent (HA) and Foreign Agent (FA; only for IPv4) are employed for location management as well as data transport. The HA is the entity that maintains location information for the host. It resides in the host home network and is responsible (when the MN is away from home) for keeping track of current location of MN by storing its CoA and tunnelling the incoming data to the current location of the MN.

Mobile IP has four particular stages as explained in RFC 3344: [1]

Agent Discovery: This mechanism is an extension of Router Advertisement protocol (specified in RFC 1256). FAs and HAs are broadcasting their own Agent Advertisement messages at regular intervals. In addition to information related to the default router, these messages carry information about care-of-addresses and a flag indicating whether it is a home agent, foreign agent or both. These messages in the next step received and examined by MNs in order to find out whether they are in the home network or the foreign network. Then the mobile node can accelerate this procedure by sending out an Agent Solicitation message instead of waiting for an Agent Advertisement.

Registration Stage: This mechanism consists of the following steps:

- If the mobile node discovers that it is in a foreign network, it sends a registration Request message to the FA to register with it. This message includes the mobile node's permanent IP address and the IP address of its home agent.

- The FA, in turn, relays the Registration message, containing the mobile node's home IP address and the IP address of the FA, to the HA of that mobile node.
- The HA receives this Registration request message, updates its mobility binding table and sends an acknowledgment to the FA.
- The FA updates its visitor list and relays the message to the mobile node.

Tunnelling Stage: As The CN knows about the permanent IP address of the mobile node, it sends all packets to this address. When the HA receives the packet, it reads the packet and checks its mobility binding table to extract the current location (CoA) of the mobile node. The HA, uses this CoA to create a new IP header, that the old IP packet is placed in the payload of the new packet. This process is called "Tunnelling" or "IP-in-IP encapsulation" [29].

The FA receives the packet and decapsulates it and finds out the mobile node's home address. Then, the FA checks its visitor list to see whether it has an entry for that mobile node. If the FA finds an entry for that mobile node, it retrieves the corresponding media address and relays the packet to the destined mobile node.

In the reverse communication, when the mobile node sends a packet to the correspondent node, it sends the packet to the FA and the FA sends the packet to the correspondent node directly. The FA gives services to the mobile node as long as the lifetime has not expired. If the mobile node wants to continue using that FA service, it should re-register with that FA.

Deregistration stage: If a mobile node wants to turn off or move to another area, which is covered by a new FA, it should drop its care-of-address by deregistration with its home address. To do so, the Mobile node sends a Registration Request with a lifetime set to zero to its HA. There is no need to deregister with the FA because the lifetime will expire and the mobile node deregisters automatically. Before the lifetime with the FA has expired, all the packets sent to the mobile node are lost because the old FA does not know the new mobile node's care-of-address. Basic operation of mobile IP is shown in Figure 2-10.

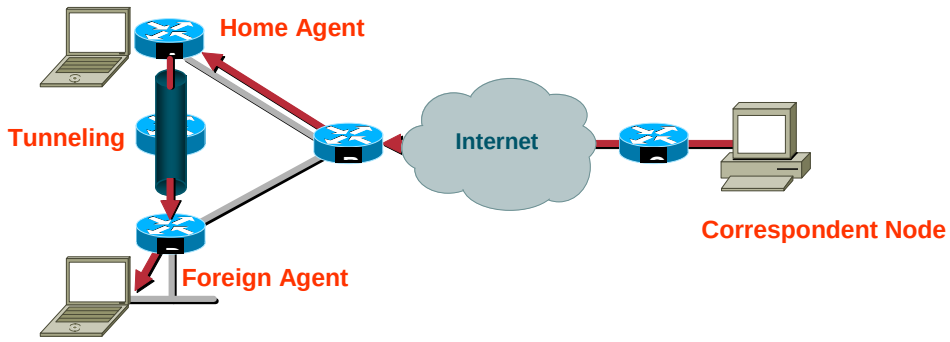

Figure 2-10: Basic operation of Mobile IP

The routing update latency can drop many packets transmitting to the mobile node. Mobile IPv6 route optimization allows direct communication between the correspondent node and the mobile node, but the packet-loss duration during handover would increase with the distance between the two nodes. Hierarchical mobile IPv6 partially solves this problem, using mobility anchor points in foreign networks to manage routing changes within their domain. Correspondent nodes contain the mobile agent's regional or hierarchical address rather than the mobile node's address. This solution reduces the duration of packet loss. Fast handover also minimizes packet-loss duration. The mobile node obtains a new address for the new access router while still connected to the old access router. The mobile node then sends the binding update to the old access router, which redirects packets to the new care-of address.

2.7. Data link based mobility (IEEE802.21)

The IEEE 802.21 [30] framework improves the network discovery by exchanging network information and helps mobile nodes decide which networks are available in their current location. This information could include link type, the link identifier, link availability and link quality etc. of nearby network links. This procedure allows the mobile node select from the available links based on the required services, QoS and probably pricing.

Handovers may occur either between two different access networks or between two different points of attachment of a single access network. In such cases

service continuity is defined as the continuation of the service during and after the handover while minimizing aspects such as data loss and break time during the handover without requiring any user intervention. The change of access network may or may not be noticeable to the end user, but there should be no need for the user to re-establish the service. There may be a change in service quality as a consequence of the transition between different networks due to the varying capabilities and characteristics of the access networks. For example if the QoS supported by new access network is unacceptable, higher layer entities may decide not to handover or may terminate the current session after the handover based on applicable policies. This specification specifies essential elements which enable service continuity.

The scope of the IEEE 802.21 (Media Independent Handover) standard is to develop a specification that provides link layer intelligence and other related network information to upper layers to optimise handovers between heterogeneous media. This includes links specified by 3GPP, 3GPP2 and both wired and wireless media in the IEEE 802 family of specifications. Handover control, handover policies and other algorithms involved in handover decision making are generally handled by communication system elements which do not fall within the scope of the IEEE 802.21 standard. Figure 2-11 shows the IEEE 802.21 architecture.

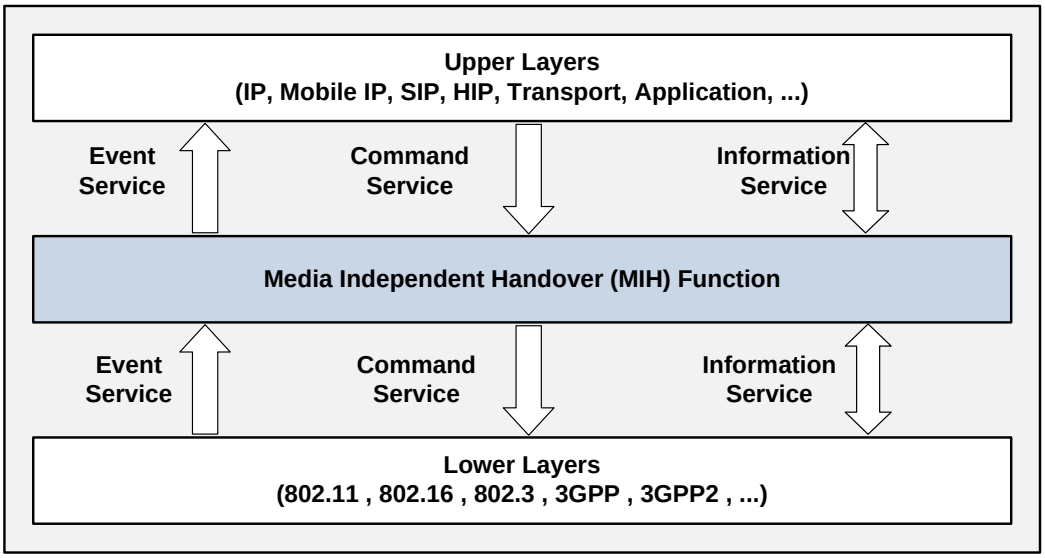

Figure 2-11: IEEE 802.21 architecture

2.8. Group mobility management

Protocols to handle mobility for a single node across different layers have been considered in the previous sections. There are some situations where a group of users (i.e. the users in a train, ship or airplane) must all be handed over to another access network within a short time span. This form of handover is called group handover (see Figure 2-12 handover scenarios, (a) single node mobility, (b) group mobility), which is the main focus of this thesis.

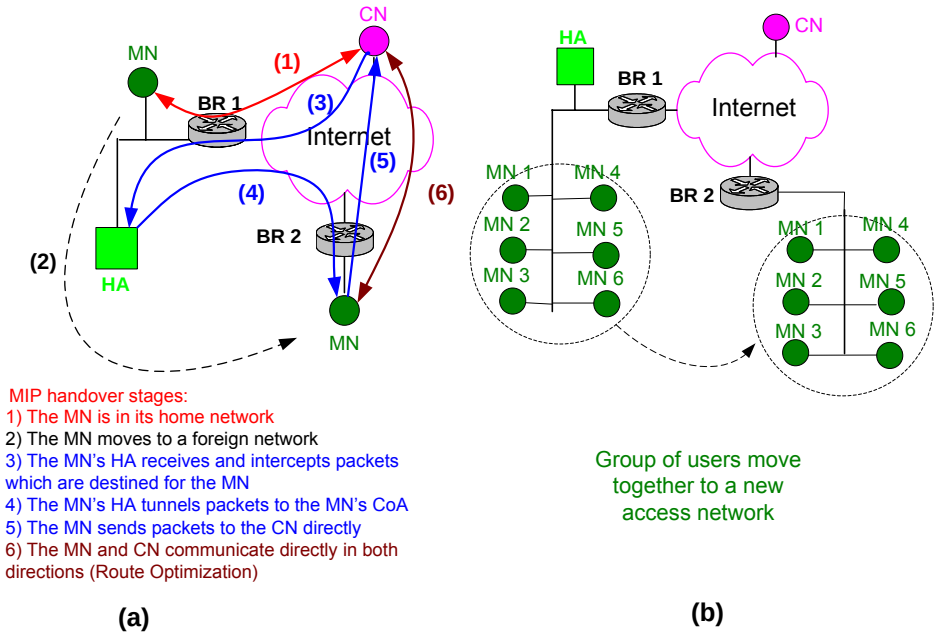

Figure 2-12: Handover scenarios (a) single node mobility (b) group mobility

In any group-handover scenario, there are two possible approaches. In the first approach, users can be handed over individually. This causes a huge amount of signalling overhead, as signalling for the handover must be sent/received by all the nodes within a short time span, causing phenomena such as a "Binding Update storm." It is therefore an ineffective way of using access networks with scarce radio resources. In the second approach, all users are considered as a unit- a complete network-and handover applies to the network as a whole. Here, all users in the mobile network have a common point of connectivity to the outside world, the Mobile Router (MR); the MR is treated as a MIP client that takes care of all mobility-related signalling. Hence, through this approach, network mobility is transparent to users. As the latter approach yields obvious advantages in terms

of handover performance, any suitable group-handover solution should be based on this concept.

In the next chapter, all existing group-handover solutions are described and analysed in detail.

Chapter 3. Multi-homing and Group Mobility Management Solutions

Before proposing solutions for the provision of group mobility in heterogeneous wireless environments, it is of paramount importance to understand existing contributions to the field, in terms of architectures, technical approaches and analytical techniques that may be applied to this work. It is therefore the intention of this Chapter to introduce existing related architectures and approaches and previously proposed analytical techniques.

3.1. Multi-homing Solutions

When a host has several interfaces and accordingly IP addresses to choose between, it is said a host is multi-homed [31]. Multi-homing offers three main benefits to hosts: it allows route recovery on failure, redundancy and load-sharing. Many attempts have been made to propose a multi-homing protocol to fulfil some of above requirements. However, at the moment defining a protocol specifies how to use several interfaces inside a mobile node or mobile network is a challenging issue.

As most of the other techniques in networking, multi-homing can be defined in different protocol stack layers and the general question is which layer is the most suitable for multi-homing? In this section, the multi-homing related works in different layers are considered.

- Link Layer Multi-homing: Transmission in the link layer is based on byte-by-byte transport over an unreliable physical layer interfaces. Byte ordering is an important issue in this layer, therefore, for preventing out-of-order delivery and also reconstructing IP and MAC addressing for different interfaces, the overhead will be increased significantly and makes this layer unsuitable for multi-homing.

- Network Layer Multi-homing: network layer solutions should be transparent to the upper layers and do not impose extra overhead and/or interference for these layers. Network layer provides a point-to-point connection and therefore the solutions in this layer are involved in network or internet infrastructure with some changes.
- Layer 3.5 Multi-homing: Host Identity Protocol [32] is a protocol defined for host mobility by decoupling the transport layer from the network layer. Multi-homing solution based on this protocol has been proposed in [33]. This solution binds the transport layer sockets to a host identifier that takes care of dynamically changing IP addresses and consequently handling the mobility and multi-homing. Recently, a HIP (Host Identity Payload) based mobility management protocol for NEMO has been proposed in [34] that reduces signalling and tunnelling overhead in IPv6-NEMO and increases the security but it suffers from weaknesses of adding a new layer to the OSI reference model and non transparency for the end users.
- Transport Layer Multi-homing: multi-homing at the transport layer is controlling multiple paths simultaneously. Unlike TCP that cannot support multi-homing some transport layer protocols like SCTP [3] and pTCP [35] have been developed to support multi-homing. pTCP control different interfaces by defining a set of modified TCP for each interface and SCTP has been discussed in section 2.5.1.
- Session Layer Multi-homing: session layer based solutions work like an interface between application and lower layers. Application sends the request to the session and based on the provided information; at the session layer decision about the suitable transport protocol for different interfaces is made[36].
- Application Layer Multi-homing: application layer is where all the information about the application and its requirements exists. At first glance it looks to be a suitable position for striping the data and gathering it again in the receiver node, but, with taking in to the account lower layer problem like head of line blocking at the transport layer and

mobility issues the overall performance of multi-homing at this layer is not acceptable.

Multiple Care of Addresses (MCoA) mechanism proposed at the IETF [37] to solve the problem of single CoA in the current MIPv6 and NEMO. MCoA supports more than one CoA registration with home network(s) and correspondent node by adding an extension to MIPv6 and configuring the tunnels. Based on MCoA mechanism in [38], a multiple tunnelling between HA and MR has been considered, with one of them can be defined as a default tunnel to take care of the packet transmission. In another study, Chio et al. [39] proposed a multi-homing mechanism type (1,2,1) - explained in section 4.2 - to support network mobility in next generation networks. Their solution is towards supporting the seamless connectivity for mobile network based on IPv6 by facilitating the network to multi-homed connectivity in the network level. Simulation results in [39] shows that two multi-homed scenario performing better handover delay but still far from achieving seamless handover in network mobility scenario.

3.2. Group Mobility Management Solutions

In any group handover scenario, there are two possible approaches. In the first approach, users can be handed over individually. This causes a huge amount of signalling overhead, as signalling for the handover must be sent/received by all the nodes within in a small time span, causing phenomenon known as a "Binding Update Storm." Individual handover is therefore an ineffective way of using access networks with scarce radio resources. In the second approach, all users are considered as a unit -a complete network- and handover applies to the network as a whole. Here, all users in the mobile network use a common point of connectivity to the outside world called the Mobile Router (MR). The MR is treated as a MIP client, which takes care of all mobility-related signalling. Hence, through this approach, mobility of the network is transparent to users. As the latter approach yields obvious advantages in terms of handover performance, any suitable group handover solution should be based on this concept.

For any group-handover solution to be practical, it must meet the following requirements in a satisfactory manner: [40, 41]

Scalability: The solution should be scalable to a considerable number of participating MNs (e.g. the number of nodes in a train, airplane or ship)

Re-use of existing protocols: If possible, the solution should only require the enhancement of existing protocols, such as MIPv6

Efficiency: The suggested solution should provide an efficient way of using radio resources by reducing the amount of signalling overhead

Minimum changes to the outside world: The suggested solution should not cause any major modifications to entities in existing networks. However, it is expected that some network entities will be added

Reliability: The suggested solution should be reliable and robust

The solution must also address the following issues, important to its applicability in the range of group mobility scenarios in heterogeneous environments [42]

Migration from one access network to another: The whole mobile network moves as a unit (network entities remain co-located), using a MR to provide Internet connectivity for nodes within the network

Joining/leaving a mobile network: MNs can freely join/leave mobile networks and are able to connect to different types of access networks

Route Optimisation: To improve handover performance and reduce traffic delays, routes to the mobile network should be optimised as efficiently as possible

Nested mobility: One or more mobile networks can be hierarchically situated below a top-level mobile network. For instance, a Personal Area Network (PAN) might join the mobile network in a train or airplane

Multi-homing/multi-access: The MR can have multi-link capabilities, thus able to use more than one access network simultaneously to assist reliability and provide application-optimised communications

In the following sub-sections, relevant group-handover solutions are analyzed and their advantages/disadvantages are addressed according to the above criteria.

3.2.1. Hierarchical Mobile IP (HMIPv6)

HMIPv6 was developed by Ericsson and INRIA and is specified in IETF RFC 4140 [19]. The HMIPv6 supports a hierarchical mobility management in order to reduce the amount of binding-update signalling to corresponding nodes and the home agent. Although the HMIPv6 focuses on mobile nodes rather than mobile networks, it may improve handover speed in mobile networks using the "extended mode".[40]

For addressing the network mobility in HMIPv6, a hierarchy of Mobility Anchor Points (MAPs) is needed. In the simplest case, this hierarchy of MAPs consists of a mobile router and a higher-level MAP. The mobile router must be configured in HMIPv6 extended mode, while the higher-level MAP may use either basic or extended mode. Due to hierarchical nature of this solution, nodes in the mobility network have three care-of addresses, one local and two regional (one belongs to the MR and the other one belongs to the higher-level MAP). All MAPs send announcement messages and the nodes in the mobile network receive these announcements and update their own binding caches; therefore, all nodes must be aware of the mobility of the MR.

3.2.1.1. Advantages and Drawbacks

In order to implement this hierarchical mobility management, some extensions to MIPv6 and "Neighbour Discovery Protocol" should be added. This solution also requires minor modifications to the mobile nodes and the home agent (only in extended mode), but the correspondent nodes remain unaffected. The rule of the MAPs is to limit the signalling outside a local domain and support fast handovers. The more hierarchical a network topology, the more efficient HMIPv6 is. Theoretically, the HMIPv6 can support very complex topologies including nested mobile networks. However, this is more a theoretical option, since many detailed questions are not solved in [19]. The approach might not scale well to a large number of hierarchies.

As previously mentioned, this solution only works for mobile nodes being aware of mobility; therefore, every node has to handle its own mobility. As a result, "Fixed" nodes are not supported. The main problem of this solution is security.

The HMIPv6 addresses many of security problems[19], such as return routability tests, but that version does not explicitly mention mobile networks.

3.2.2. Prefix Scope Binding Updates

The Prefix Scope Binding Update solution uses Mobile IPv6 Binding Update, but associates a care-of-address with a prefix instead of a single address [43]. The main assumption in this solution is that all nodes in a mobile network share a common prefix and the MR's ingress interface is configured with the mobile network prefix. In this solution, the Mobile IPv6 Binding Update has been modified to have a new sub-option, containing the mobile network prefix field. The binding-cache management in the MR's home agent, as well as in the correspondent nodes, should also be slightly modified compared to MIPv6 (particularly in searching for entries) so that the address comparison considers prefixes. This modification in correspondent nodes is particularly important because routing optimisation can only be implemented if the correspondent node explicitly supports Prefix Scope Binding Updates. By implementing the route optimisation, it is possible to address the Binding Update Storm problem of MIPv6 and reduce the amount of Binding Update signalling as only one Binding Update has to be sent to every Correspondent Node in the entire mobile network [40].

In this solution, the home agent uses the proxy neighbourhood advertisements to intercept all packets sent to the mobile network prefix, and then forwards them to the MR’s CoA. Therefore, when the MR acquires a CoA, using this CoA will be enough for all packets destined to the nodes in the mobile network to reach their final destinations. In this case, all packets destined to nodes in the mobile network are forwarded to the care-of address of the MR.

3.2.2.1. Advantages and Drawbacks

The Prefix Scope Binding Update approach is not designed to address the following issues[40]:

- It cannot provide Multi-homing because the mobile network attaches to the Internet using only one egress interface.

- This solution addresses only local fixed nodes. The IETF Internet-Draft [43] does not address problems related to mobile nodes.
- Nested networks are not supported in this approach.

Taking into account all these restrictions, very simple mobile networks, including only one mobile router with only one direct connection to the Internet, could be considered in this approach. There might be practical scenarios for this simple case, but a more general approach, which provides support for visiting mobile nodes and multi-homing, is more desirable.

3.2.3. Mobile Router Tunnelling Protocol

The third solution of moving network scenario is described in [44]. This solution is based on a bi-directional tunnel between the MR and its home agent. Apart from some modifications to the packet forwarding implementations, this method uses Mobile IPv6 without any modification. Generally speaking, MR has two different modes in this solution:

- Fully Enabled Mobile Router: The mobile router (MR) uses a dynamic routing protocol, acts like a normal fixed router in the Internet and redirects traffic towards its home agent by means of a dynamic routing protocol. The dynamic routing protocol updates the routing state between the home agent, mobile router and gateways to the Internet
- Consumer Mobile Router: When the MR is not at home, its home agent uses static routes for a restricted set of links behind the MR. These static routes are pre-configured

Regardless of which mode the MR uses, the receiving packets are examined by the MR's home agent and are encapsulated and tunnelled to the MR's CoA. In order to have this method to work properly, both the mobile router and its home agent should be aware of tunnel establishment and know that packets for the mobile network must be routed through that tunnel. In order to do so, some signalling information should be sent between the MR and its home agent. These signalling messages could be either implicit (meaning that no changes to the Mobile IP messages are required) or explicit. For explicit signalling, an optional

"mobile network option" is defined in order to specify prefix mappings, which may be included in Binding Updates and Binding Acknowledgments [40].

3.2.3.1.Advantages and drawbacks

Mobile Router Tunnelling Protocol like Prefix Scope Binding Updates uses the prefix option, but there are three main differences between these two solutions. Firstly, the current version of Mobile Router Tunnelling Protocol does not support any routing optimisation to and from the mobile network (Route Optimization issues are under investigation). As a result, no binding updates are sent to the correspondent nodes. Secondly, Mobile Router Tunnelling Protocol supports mobile nodes. These mobile nodes can attach to the mobile network using Mobile IP features and can get a care-of address of the link inside the mobile network. Finally, nested mobile networks are possible in this solution because a mobile router can insert several prefixes on the home link.

As a dynamic routing protocol can be used inside the mobile network, as well as on the home network, multi-homing could be possible in this solution (although it is not considered in [44]).

Another important advantage of this solution is that neither Mobile IP nor routing protocols should be modified, and therefore no additional security problems occur. In this approach, a considerable part of the problem is shifted from Mobile IP to the dynamic routing protocol i.e. it is up to the routing protocol to decide whether a route may be injected in the home link, and up to existing Authentication, Authorization and Accounting (AAA) mechanisms to decide whether a mobile node may attach to a mobile network.

The main problem is that networks with fast topology changes, such as ad-hoc networks, cannot be supported. This problem stems from the fact that, the Mobile IP is only used to establish the tunnel between the mobile router and its home agent and mobility is handled by the chosen routing protocol on the home link. Therefore, if the routing protocol converges slowly, frequent handovers cannot be handled by this solution.

3.2.4. Optimised Route Cache Management Protocol for Network Mobility (ORC)

This solution is the most recent solution for network mobility. This solution uses the bi-directional tunnel between MR and HA [2, 45] and some other characteristics of the previous solutions such as prefix-scoped binding updates. The new features of this solution, compared with previous solutions, are:

- The home address of the mobile router is assigned to the ingress interface of the Mobile Router (and not the egress interface)
- There is a two-step approach in the search algorithm for the binding cache
- The "Prefix Delegation" concept is introduced for the assignment of the mobile network prefix

The ORC protocol also introduces a new architectural component called the Optimized Route Cache (ORC) router, which deals with routing messages. If this router is used relatively close to the CN, route optimisation can be achieved without any modification to the CN.

By using ORC routers, some important advantages can be obtained. As previously mentioned, route optimisation can be deployed without modification to the CN by implementing an ORC router close to the CN--even as the next-hop router. In this case, the CN does not need to know anything about the changes. As CNs can be present anywhere in the Internet, these ORC routers can also be anywhere in the Internet to take advantage of this feature[40].

3.2.5. Comparison

In this section, all the above mentioned solutions (HMIPv6, prefix scope binding updates, mobile router tunnelling protocol and ORC) are compared in order to find the most suitable solution for group mobility scenarios in heterogeneous environments.

The HMIPv6 approach can support visiting mobile nodes, route optimisation and nested mobile networks, but cannot support local fixed nodes and multi-homing.

The Prefix Scope Binding Updates solution supports local fixed nodes, route optimisation between mobile network nodes and any CN in the Internet, but it cannot support visiting mobile nodes or nested mobile networks. The Mobile Router Tunnelling Protocol supports local fixed nodes, visiting mobile nodes and nested mobility. It also supports the running of a dynamic routing protocol between MR and HA, which makes this solution very scalable.

The ORC protocol is the latest solution provided for network mobility management and can support most network mobility issues such as nesting, RO, secure RO and multi-homing. This solution, however, completely depends on the deployment of ORC routers throughout the Internet, requiring major changes to the Internet.

As a result, Mobile Router Tunnelling Protocol is the most complete solution for group mobility in heterogeneous environments. This solution, which is an extension of the MIPv6 tunnelling approach, was chosen by the IETF's NEtwork MObility (NEMO) working group as the most practical solution for group handover. According to the NEMO working group, the group mobility problem can be approached in two different phases, the "NEMO Basic Support" solution and the "NEMO Extended Support" solution. The Basic Support solution fulfils the following important goals [41, 42]. Firstly, the solution provides session continuity throughout the MN's changes in points of attachment to the Internet during handover which is essential to the seamlessness of handovers, In other words, handovers to different access networks are transparent to the users. Secondly, the solution provides reachability for MNs, regardless of their current points of attachment to the Internet. To meet this objective, the Basic Support protocol allocates a globally available IP address to each node in the mobile network[2].

The NEMO Extended Support solution handles issues such as route optimisation and multi-homing, at the cost of considerable complexity to the scheme. In the next section, group mobility scenario, which appropriately reflects the complexities and implementation requirements of the NEMO Basic Support protocol, is presented. In section 4.1, multi-homing issues of NEMO and possible solutions were addressed.

3.3. NEtwork MObility (NEMO)

There are some situations where a group of users (i.e. the users in a train, ship or an airplane) must all be handed over to another access network within a short span of time. This form of handover is called group handover. As seen in the previous section 3.2, the most suitable solution for network mobility is NEMO. NEMO has been nominated as the most complete solution for group mobility in heterogeneous mobile networks. In this section the detailed operation, tunneling configuration, strengths and drawbacks of this protocol will be addressed.

3.3.1. NEMO Components

NEMO is an extension of Mobile IPv6 that provides connectivity while an entire network is changing its point of attachment to the Internet. Based on NEMO, mobility functionality moves from mobile nodes to a mobile network's router (namely MR) and all users are considered as a unit and handover applies to the network as one. The Mobile Router (MR) is treated as MIP client and takes care of all network mobility related signalling. Hence through this approach, the mobility of the network is transparent to the users.

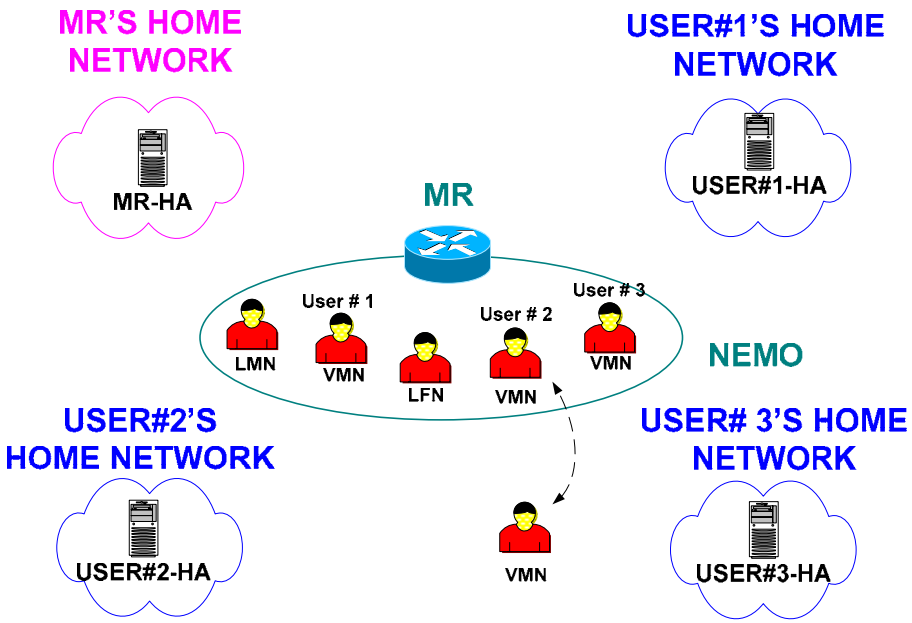

Figure 3-1: NEMO components

The NEMO basic support solution components as shown in Figure 3-1 are as follows [2]:

- Mobile Router (MR): The MR provides an external gateway for the nodes in the attached network
- MR's Home Network: This network to which the MR belongs
- MR's Home Agent: The router in the MR's Home Network, which is responsible for MR's network mobility
- Local Fixed Nodes (LFNs): Fixed nodes in the MR's network. These nodes are unable to change their point of attachment to the MR's network. LFNs are mobility unaware nodes, meaning that they do not have any mobility software running on them
- Local Mobile Nodes (LMNs): Mobile nodes in the MR's network. These nodes are able to change their point of attachment to the MR's network, but they are unable to leave the MR's network
- Visiting MNs (VMNs): Mobile nodes in the MR's network. These nodes are capable of joining/leaving the MR's network when necessary. VMNs are mobility-aware nodes, meaning that they must have mobility software such as MIPv6 installed and running
- User's Home Network: The network that the user is subscribed to. This network is responsible for maintaining the user's profile, billing, authentication, traffic monitoring and other issues. It should be noted that different users might have different home networks
- User's Home Agent: The router in the user's Home Network that is responsible for the user's mobility

In the MR-HA bidirectional tunnelling approach, which is essential for the functioning of the NEMO Basic Support Protocol, the MR acquires one or more IPv6 (it has to be IPv6 in NEMO Basic Support Protocol) prefixes from its home network. Then the MR assigns IP addresses to LFNs/LMNs from its IPv6 prefixes. LMNs/LFNs use these IP addresses as their permanent IP addresses and register them with the MR's HA. These IP addresses stay the same and will not change.

When a VMN joins the MR's network, the MR assigns an IP address (based on the prefix) to the VMN, which the VMN uses as its CoA. The VMN then sends a Binding Update (BU) to its home network via the MR. On receiving the BU, the user's HA updates its binding cache, replies with an acknowledgement. This CoA will stay the same as long as the VMN is in the MR's network.

3.3.2. Tunnelling Configuration

In MIP[1], IP encapsulation is used to carry the packets from CN to the MN. The CN transmits the packets to MN-HA which knows the current location of MN and the MN-HA in an IP-in-IP encapsulation forwards the packet towards the MN. At the MN a decapsulation process will be performed to extract the original packets. Packet encapsulation is based on data encapsulation or data hiding in OSI reference model. Application data should pass through the network layers to add relevant header and/or trailer to the received packet from upper layers to communicate with the other end.

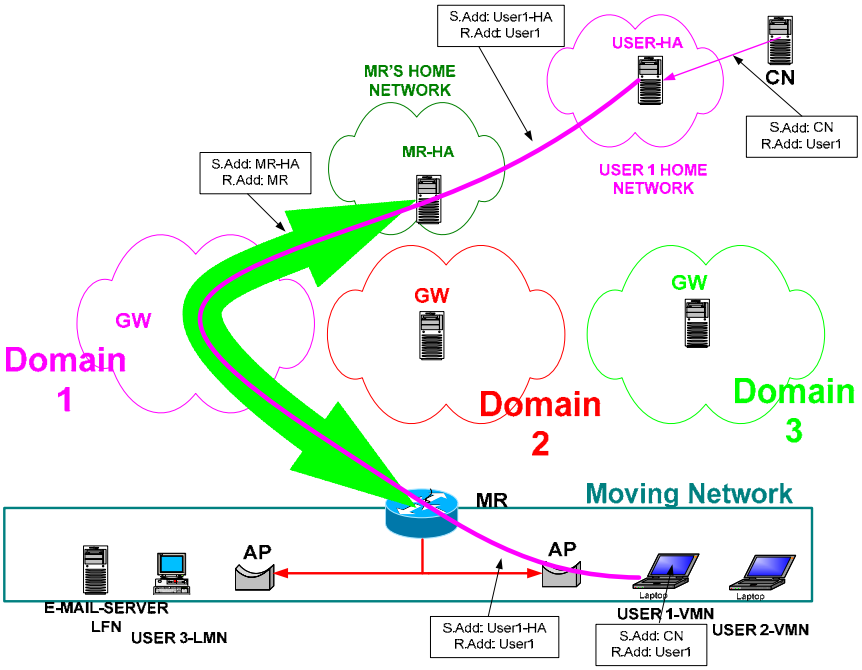

Figure 3-2 Sender and receiver IP address fields in NEMO when CN is sender

NEMO[2] is a developed case of Mobile IP which can handle data transmission using two different tunnelling mechanisms. In NEMO a VMN gets a CoA from the MR's network. This CoA has a prefix of the MR and will not be changed while the VMN is connected to the MR. If the CN wishes to communicate with the MN in the moving network the following process should be done:

- CN is aware of the MN's IP address that belongs to the home network's domain and will place this address in the destination IP header field of packet.
- The destination IP address has a prefix of the MN-HA and the packet is transmitted to the MN-HA.
- The MN-HA knows the CoA of the MN. A packet encapsulation with MN-HA and MN-CoA in source and destination address fields will be formed.
- As MN-CoA has a prefix of the MR, in the next stage this packet should be received by the MR-HA.
- The MR might be out of the home network. In that case, the MR-HA which has the current IP address of the MR tunnels the packet again and sends it to the current location of MR. Source and destination IP addresses in this IP header are MR-HA and MR-CoA respectively.

Figure 3-2 shows the source and destination IP addresses in each part of transmission when the CN is a sender. The reverse transmission from VMN to CN is formed by swapping the sender and receiver addresses in Figure 3-2.

When the MR is away from its home network, it obtains a new address (primary CoA) and registers this new CoA with its home agent. When the new MR CoA registrations with its home agent finished, all traffic to visiting nodes within the mobile network is routed to the MR's home agent and then double tunnelled (using IP-IP encapsulation) to the MR. As the MR roams through different domain and performs a hard handover, new CoA will be allocated to the MR that again must be registered with the MR-HA. The double tunnel is formed between the following objects: (see Figure 3-3)

- Outer tunnel: from MR's home agent to MR

- Inner Tunnel: from user's home agent to the VMN

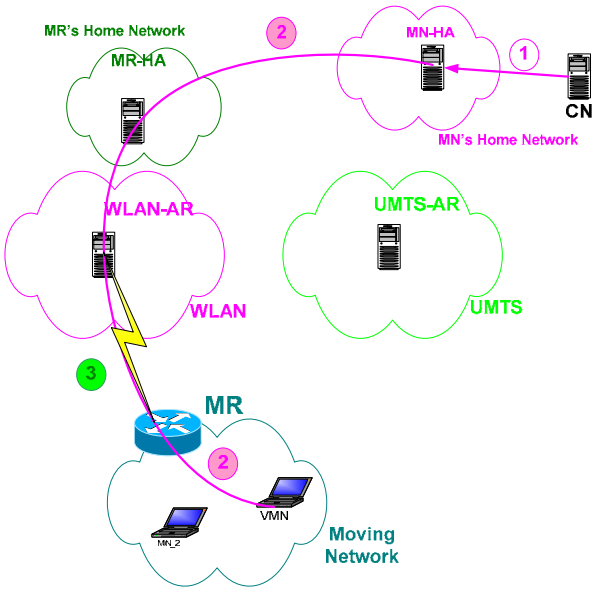

Figure 3-3: IP traffic between a VMN and a CN using NEMO;1: Original data path, 2: Inner tunnel, 3: Outer tunnel

Figure 3-4 illustrates the data path from a CN to a VMN node in the mobile network:

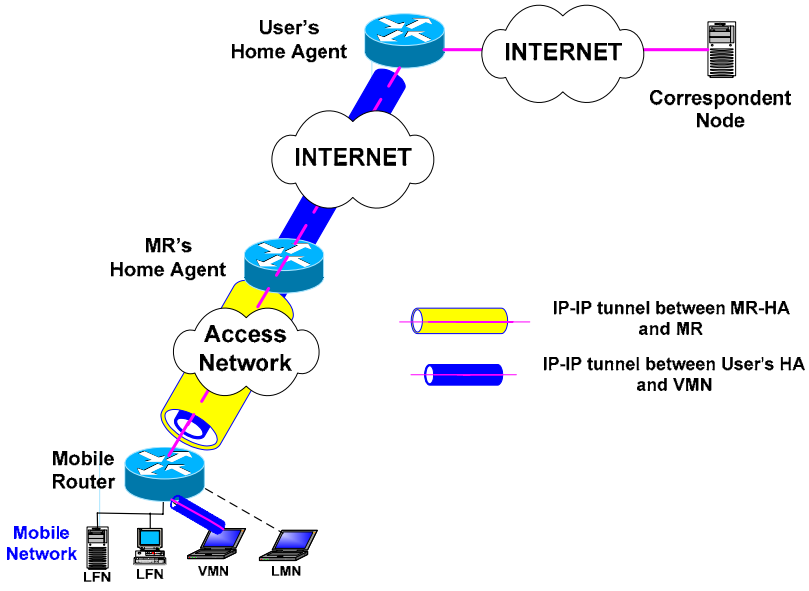

Figure 3-4: Data path for a VMN

The traffic to fixed/mobile nodes within the mobile network is routed to the MR's home agent directly and then gets tunnelled (using IP-IP encapsulation) to the MR.

Figure 3-5 illustrates the data path from a CN to a LFN/LMN node in the mobile network:

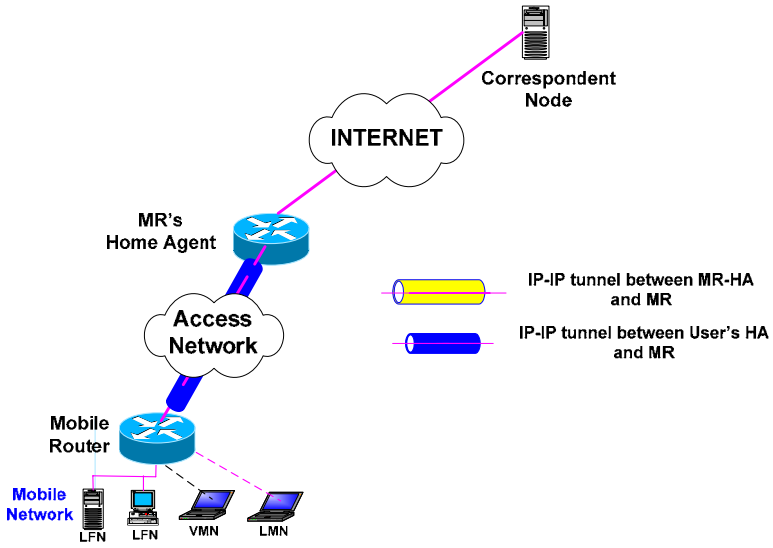

Figure 3-5: Data path for a LFN/LMN

3.4. Chapter Summary and Problem Definition

In this chapter, all existing group-mobility solutions have been compared and the IETF's NEtwork MObility (NEMO) working group's choice, Mobile Router Tunnelling Protocol, is explained in detail. This solution, as is suggested by the NEMO working group, does NOT support group-mobility in heterogeneous wireless environments and multi-homing features. In order to address this issue, a novel group-mobility solution, which is an extension of the NEMO Basic Support protocol, is introduced in the next two chapters.

A well-known weakness of NEMO structure is vertical handover[2] that can cause service disruption and disconnectivity during an end-to-end communication. Also, single point of failure in NEMO architecture is another source of distraction in the communication link. Multi-homing can tackle the problem of single point of failure which can be achieved at different layers. At the application layer, the firewall proxy services can provide this functionality.

At the transport layer, session allows binding multiple IP addresses at each end point. The network layer approaches to multi-homing are router-based and, finally, in data link and physical layers multi-homing can be implemented by manipulating MAC address to provide virtual server functionalities.

As explained before, SCTP is a transport layer protocol with the ability of multi-homing that can tackle the problem of single point of failure. This facility enables more than one connection via different interfaces and transmission paths between two end nodes.

In the proposed architecture in the next chapter, the MR and the MR-HA has been selected to run multi-homed SCTP protocol, where the outer tunnel is performing. Running SCTP protocol on these multilayer routers (MR and its peer MR-HA) gives the opportunity of having another end-to-end protocol at the bottleneck of the network that always has to deal with air interface issues like unreliability and high packet error-rate. On the other side based on the mSCTP [20], having more than one connection between MR and MR-HA via different wireless network technologies or BSs can provide seamless vertical or horizontal handovers respectively. The other features that can be achieved are load balancing and load sharing that are out of scope of this thesis.

Chapter 4. nSCTP: Seamless Handover for Moving Network

As discussed in the previous chapter NEMO suffers from a well-known weakness, connection disruption while the mobile device migrates to a new coverage area. That is due to the delay for obtaining a new address from the migrated cell and registering this address with its home agent and finally resuming the transmission towards the new address/location.

The conclusion of the previous chapter pointed out the necessity of having more than one connection at the wireless part of the NEMO structure. These parallel links will be dealt with mobility issues and also working as a "backup link(s)" at the part of the network that must handle high error-rate and interference and other consequences of the wireless media. Enabling multi-homing in the NEMO scenario, apart from solving the ubiquitous access by defining an alternative connection, could enhance the reliability and facilitate the load balancing and load sharing within the communication system.

This chapter presents a new protocol to enhance the connection robustness by providing seamless global mobility, increasing fairness and avoiding congestion collapse for moving networks. The new protocol is a transport-layer tunneling protocol based on Stream Control Transmission Protocol (SCTP) [3]. The new protocol provides a virtual reliable connection in the wireless channels to address the challenges of high bit error-rate, limited bandwidth and mobility management.

Transport layer tunneling is a method for building a virtual circuit, by aggregating flows between two nodes or routers and treating them like a single connection. TCP tunnels can be deployed by Internet service providers and/or mobile network providers on point-to-point links to take advantages attributes of them and offer better service. TCP tunnel in this category has been widely used in several tunneling applications such as SSH[46], VTun[47] and HTun[48].

Despite the efficiency of TCP trunking there are some well-known weaknesses that are mentioned in [49]. Firstly, stacking two TCP connections on top of each other increases the RTT for an end-to-end connection also causes some problems when the packet loss happens inside the tunnel. TCP is strictly reliable and retransmits the lost packets unlimitedly, while this could not be efficient in some cases especially about the UDP flows[50]. Secondly, in the wireless access networks where connections need to deal with huge a percentage of packet loss and handover, TCP tunneling does not seem to be a good solution.

In this chapter, firstly the benefits of multi-homing in NEMO are outlined. Then, all possible multi-homing configurations for NEMO are explained and their practicalities evaluated against implementation criteria. The important criteria for group mobility scenarios are discussed and most suitable configuration for group handover scenario is presented and this selection is justified. In transport layer tunneling, SCTP/IP encapsulation/decapsulation have been defined. The data path and signalling issues for proposed scenario have been discussed. Finally, the outcome of this chapter is introducing nSCTP (NEMO-SCTP) protocol with the help of transport layer tunneling and data hiding algorithms that forms the basis of the investigations presented in this chapter.

4.1. Benefits of multi-homing in NEMO

4.1.1. Permanent and Ubiquitous access

As implied before, in a mobile communication environment issues such as handover and high error-rate, will caused a mobile router with only single interface not to be efficient in most of the cases. Therefore, there is a need for a MR with several interfaces to provide ubiquitous access to the Internet that can be deployed everywhere and provide sufficient QoS for the nodes in the mobile network. For example, flow of traffic should be redirected from one interface (e.g. WLAN) to (an)other interface(s) (e.g. UMTS) due to the loss of connectivity or change of the network conditions such as available bandwidth and other QoS parameters. In addition, the handover entity should be able to select the most appropriate set of network interface(s) for the MR depending on

network conditions and the user's required QoS. Hence, multi-homing is an essential feature of any scenario in heterogeneous wireless environments.

4.1.2. Load sharing

There are situations in which it would be advantageous if the traffic load is spread among several routes in order to improve QoS parameters such as end-to-end delay, bandwidth, jitter, etc. For instance, if the voice part of a video clip uses a UMTS access network, as it provides less delay, and the video part of the traffic uses a WLAN access network, as it provides more bandwidth, a more effective use of resources can be achieved. Therefore, load sharing can provide many benefits for scenarios in heterogeneous wireless environments.

4.1.3. Reliability

The MR in NEMO provides connectivity to the outside world for all the nodes inside the mobile network; lose of connectivity to the Internet for the mobile router means all the nodes in the mobile network lose connectivity. As a result, the reliability of the MR's connection to the Internet is essential.

Mobile routers can be used to improve connection reliability and robustness even when implemented over access edge by enabling connection redundancy to the mobile router's home agent. In that case the mobile nodes become client for a virtual service provider, which does not take part in the actual access technology.

4.1.4. Aggregate bandwidth

Depending on the user's/application's required bandwidth, the MR might have to increase the available bandwidth by using several interfaces to meet the demand. Therefore, aggregate bandwidth is an important issue for NEMO scenario, so that possibly heavy traffic could be handled in some circumstances. At the presence of multi-homing the alternative link that in normal traffic stays in the idle mode can switch to active condition to carry some part of the traffic from the same or a different access point.

All the above benefits can be achieved by the application of multi-homing in moving networks or in any scenarios in a heterogeneous wireless environment.

4.2. Multi-homing Configurations for NEMO

As stated in [42], the NEMO Basic Support solution does not support multi-homing but implementing this feature is not prevented in the context of NEMO. In the following section possible configurations to enable multi-homing for a network in motion were studied and based on the required criteria the chosen configuration to be followed in this thesis is addressed.

4.2.1. Possible Configurations

As defined in [42], multi-homing occurs when there is more than one point of attachment between the mobile network and the Internet. This situation can arise when either [51] :

- The MR has multiple egress interfaces; and/or
- The mobile network has multiple MRs; and/or
- The mobile network has associated multiple HAs; and/or
- Multiple global prefixes are available in the mobile network

According to [51], there are eight configurations in which mobile networks can be multi-homed. These configurations are as follows:

1. Single MR, Single HA, Single MNP (Mobile Network Prefix) (1,1,1)
2. Multiple MR, Single HA, single MNP (n,1,1)
3. Single MR, multiple HA, single MNP (1,n,1)
4. Single MR, single HA, multiple MNP (1,1,n)
5. Single MR, multiple HA, multiple MNP (1,n,n)
6. Multiple MR, single HA, multiple MNP (n,1,n)
7. Multiple MR, multiple HA, single MNP (n,n,1)
8. Multiple MR, multiple HA, multiple MNP (n,n,n)

In RFC 4980[51], all these configurations and their related issues, which should be considered in order to implement each particular configuration, are explained in detail. It is worth noting that in all these configurations, a bi-directional tunnel

must be established between each pair of Home Address/Care-of-Address to provide multi-homing.

4.2.2. Important Criteria in Multi-homing Configurations

To implement multi-homing in NEMO, some important criteria for all eight configurations are highlighted in RFC 4980[51] which are summarised in this section:

- **Fault Tolerance:** This is one of the benefits of multi-homing. In order to provide this feature, a set of tasks need to be done, including failure detection, path exploration, path selection and re-homing.
- **HA Synchronisation:** In mobile networks with several HAs, a single MNP is registered at different HAs. These may cause a problem in the routing infrastructure as a whole, if the HAs are located in different administrative domains. Two cases can be considered:
  - Only one HA actively advertises a route to the MNP; or
  - Multiple HAs at different domains advertise a route to the same MNP.
- **MR Synchronisation:** In a mobile network with several MRs, the different MRs need to be synchronised in order to reach common decisions, such as:
  - Advertising the same MNP in the mobile network with several MRs.
  - One MR relaying the advertisement of the MNP from another failed MR in the (n,x,n) mobile network.
  - Relaying between MRs everything that needs to be relayed in the (n,x,x) mobile network (e.g. data packets).
- **Prefix Delegation:** In a mobile network with one MNP, the same MNP must be advertised to the MNs through different paths. This would be an issue when several HAs and/or several MRs exist in a configuration.

- **Multiple Bindings/Registrations:** Any MR with multiple CoAs should bind its CoAs to the same MNP. This a general issue for all mentioned configurations (even for a single mobile IP node).
- **Source Address Selection:** In mobile networks with multiple MNPs, MNs are configured with multiple addresses. Source-address selection mechanisms are needed to decide which address to choose.
- **Loop Prevention in Nested Mobile Networks:** When a multi-homed mobile network is nested within another mobile network, it can result in complex topologies. For instance, a nested mobile network may be attached to two different root-MRs; thus, the aggregated network no longer forms a simple tree structure.
- **Prefix Ownership:** When a network with multiple MRs splits (i.e. the two MRs split themselves up), MRs on distinct links may attempt to register the only available MNP. This cannot be allowed, as the HA has no way of knowing which node with an address configured from that MNP is attached to which MR. A mechanism must be introduced for the MNP to either be forcibly removed from one (or all) MRs, or the implementers must not allow such a split.
- **Preference Settings:** When a mobile network is multi-homed, the MNs are able to enjoy the benefits of multi-homing, such as choosing among available paths based on cost, transmission delays, bandwidth, etc.

A mechanism that allows the MN to indicate its preference for a given traffic is desirable. In addition, there may also be a need to exchange information between the MRs and the MNs. This is a general problem in the sense that any IPv6 nodes might influence the routing decision of the upstream routers.

4.2.3. Selected Configuration

Among the eight configurations mention in subsection 4.2.1, the first one, (1,1,1), would be the most suitable choice for moving network as it provides all the required benefits (i.e. ubiquitous access, load sharing, reliability and aggregate bandwidth) and has less complexity and fewer issues compared with other configurations. In this configuration, the mobile router has multiple

physical interfaces and each of these interfaces has a corresponding CoA. A bi-directional tunnel exists between each CoA and the HA (shown in Figure 3-3).

As in the selected configuration only one HA exists, issues such as: "Re-homing", "Ingress Filtering", "HA Synchronisation" and "Prefix Delegation", which are discussed in 4.2.2, are not relevant. Also as there is only one MR in this configuration, the issues such as: "MR Synchronisation" and "Prefix Delegation" do not need to be addressed. Furthermore, there is only one MNP and "Source Address Selection" is not an issue to consider.

For the sake of simplicity, the nested mobile networks are not considered in this thesis. As a result, issues such as "Loop Prevention" in Nested Mobile Networks and "Prefix Ownership" are not relevant issues.

4.3. Transport Layer Tunnelling

The current NEMO structure suffers from some distinguished weaknesses such as vertical handover latency which causes disconnectivity and service disruption during the handover, lack of some features like multi-homing [51] and load balancing that have not been addressed in the NEMO basic protocol architecture.

As explained in section 2.5.1, SCTP is a transport layer protocol with the ability of multi-homing. This facility provides more than one communication path via different interfaces between two end nodes. As transport layer solutions are end-to-end, therefore, SCTP seems to be necessarily run at the both ends (CN and User1-VMN in Figure 3-2). This solution is feasible but requires more than one interface at the end nodes, which cannot be achieved easily. On the other hand, having multi-homing in the reliable parts of network that are not involved in mobility issues and air interface instability adds additional overhead on these parts of networks and end nodes. In order to solve the above weaknesses a novel transport layer tunnelling and mobility protocol has been presented in this chapter. The basis of this new protocol is rerunning multi-homed-SCTP at the MR and the MR-HA, where the outer tunnel is performing (see tunnelling configurations, section 3.3.2). Running SCTP protocol on these multilayer routers (MR and its peer MR-HA) gives the opportunity to have another end-to-

end protocol exactly at the bottleneck of the network that always has to deal with the unreliability and high packet error-rate. On the other side having more than one connection between MR and MR-HA via different wireless network technologies or BSs can provide seamless vertical or horizontal handover respectively.

In order to activate multi-homing in NEMO scenario, two tunnels that need to be established are identified:

- Router/Host tunnelling: this tunnel is bidirectional, between MN-HA and MN. The tunnel is named inner tunnel and provides a point-to-point link based on IPv4 or IPv6 at the network layer. IP encapsulator and IP decapsulator are the modules of this tunnel which are explained in the next section. The configuration of this particular tunnel will be setup at the time that the MN joins to the moving network and will not be changed until the MN leaves the network.
- Router/Mobile Router tunnelling: this is the second bidirectional tunnel performing between MR and MR-HA. These routers should be able to process the transport layer data. SCTP/IP encapsulator and decapsulator are the modules of the tunnel which are explained in the remainder of this section. The tunnel configuration will be changed when the mobile router changes its point of attachment to the network or a new BS detects by MR interfaces.

4.3.1. IP Encapsulator

The default encapsulation process used in Mobile IP is called IP Encapsulation within IP, defined in RFC 2003 [29] and commonly abbreviated IP-in-IP. It is a relatively simple method that describes how to take an IP datagram and make it the payload of another IP datagram. In Mobile IP, the new headers specify how to send the encapsulated datagram to the mobile node's care-of-address.

The encapsulation of an IP datagram in an IP is shown in Figure 4-1.

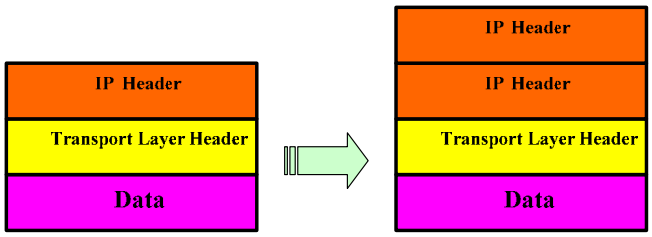

Figure 4-1: IP-in-IP Encapsulation

The capsulator besides adding an IP header has to deal with some more complex issues, such as packet fragmentation which is general effect of increasing the size of packets. Maximum Transmission Unit (MTU) is the largest physical packet size that a network can transfer. Any messages larger than the MTU are divided into smaller packets before being sent. There are some static and dynamic solutions for this issues that some of them are explained in RFC 4459 [52].

4.3.2. SCTP/IP Encapsulator

SCTP/IP encapsulator has more complexity in comparison to the IP encapsulator as it should take care of an end-to-end multi-homed connection. The two routers which are involved in this process (MR and MR-HA) besides support of multilayer protocols must uphold the SCTP. In this scenario, the multilayer router received the IP encapsulated packets from MN-HA (or MN, depending on the data direction) and employed a new transport layer over the received packets. On the received packet at the router, depending on the source and destination addresses on the top of IP header, decision between routing or encapsulation and routing should be made. In the case of encapsulation, SCTP header and IP header will be added to the received packet and finally transmitted to the appropriate port. The algorithm for this scenario is presented in Figure 4-2 and the outcome of this algorithm depicted in Figure 4-3.

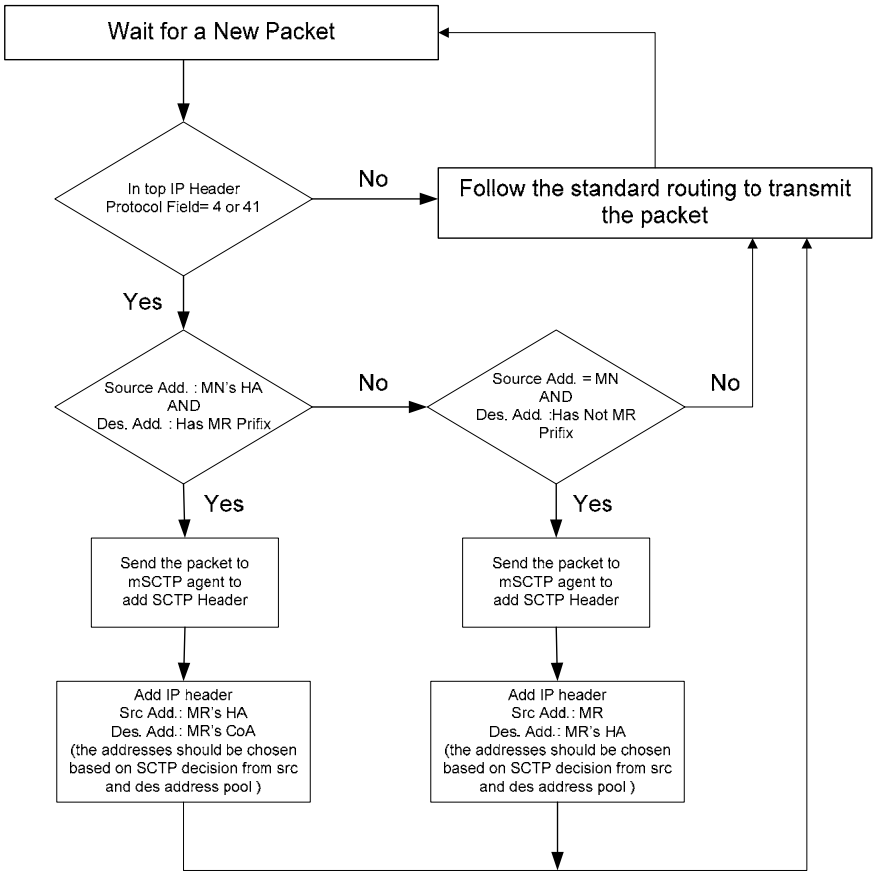

Figure 4-2: SCTP/IP encapsulation mechanisms for ongoing flow under nSCTP structure

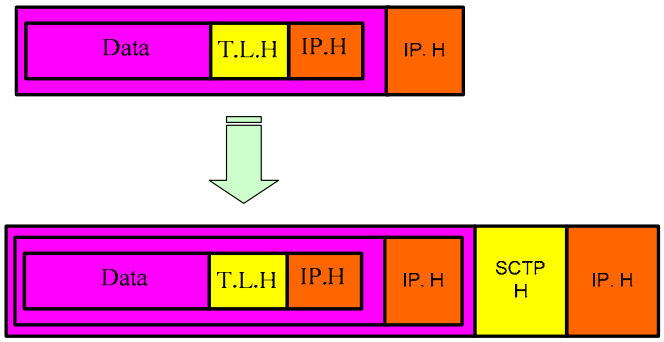

Figure 4-3: SCTP/IP Encapsulation and protocol stack in nSCTP outer tunnel

Encapsulation is configured based on the multi-homing feature of SCTP. Source and destination IP address in the created IP header, can be different between two consequent packets and this dependents on the primary link (or address) chosen by SCTP. The MR and MR-HA can have different interfaces, therefore, all the combinations in the form of binomial distribution are acceptable. The SCTP

signalling and handshaking are needed to check the availability and the QoS (not support at the moment) of the available links to decide about changes over to a particular path.

4.3.3. IP Decapsulation

Decapsulator node or router should extract the original packet from received encapsulated packet and remove the IP header, and then process the original packet for next hop routing.

In the IPv4 header there is a "protocol" field to identify the next level protocol or the next encapsulated protocol. This is an 8-bit field as described in [53] which has been changed to "Next Header" in IPv6 header as explained in [54].

Decapsulation process is summarised in the following steps:

- Considering the received packet to realise the type of encapsulation by checking the source and destination address and verifies the configured tunnel interface
- Reassembling the packet if it has been involved in fragmented because of shortage of MTU
- Removing the IP header and submit it for further process

The decimal value 4 and 41 depends on used IP version for "protocol" field in IP header shows that the received packet is potentially a tunnelled packet and needs to be sent through decapsulation process. The decapsulator discards the top IP header and checks the next IP header to pass the extracted packet through relevant port. IP decapsulator module should be run on the receiving node such as receiving VMN in the moving network or on the MN-HA when the CN is a receiver. The reverse direction of tunnelling in Figure 4-1 shows the performing of IP decapsulator.

4.3.4. SCTP/IP Decapsulator

The received SCTP/IP encapsulated packet should be decapsulated for extracting the original data. At this stage two header layers must be processed and discarded. The process of SCTP/IP decapsulator has summarised in algorithm

shown in Figure 4-4. If a packet received at MR or MR-HA and if the protocol field of top IP header is 132, means the next used protocol is SCTP. In this case, the next IP header should be considered, if the protocol field of that header is 4 or 41 (depends on the version of IP) shows that the packet has a double layer tunnelling. With respect to the decapsulation process the IP header is removed, the SCTP header is considered to meet the conditions of end-to-end protocols and the appropriate acknowledgments are sent to the source of the SCTP packet. If the packet is valid and has no error, the SCTP header is removed and transmitted to the next hop by looking to the top destination address. The opposite direction of arrow in Figure 4-3 shows the results of SCTP/IP decapsulator.

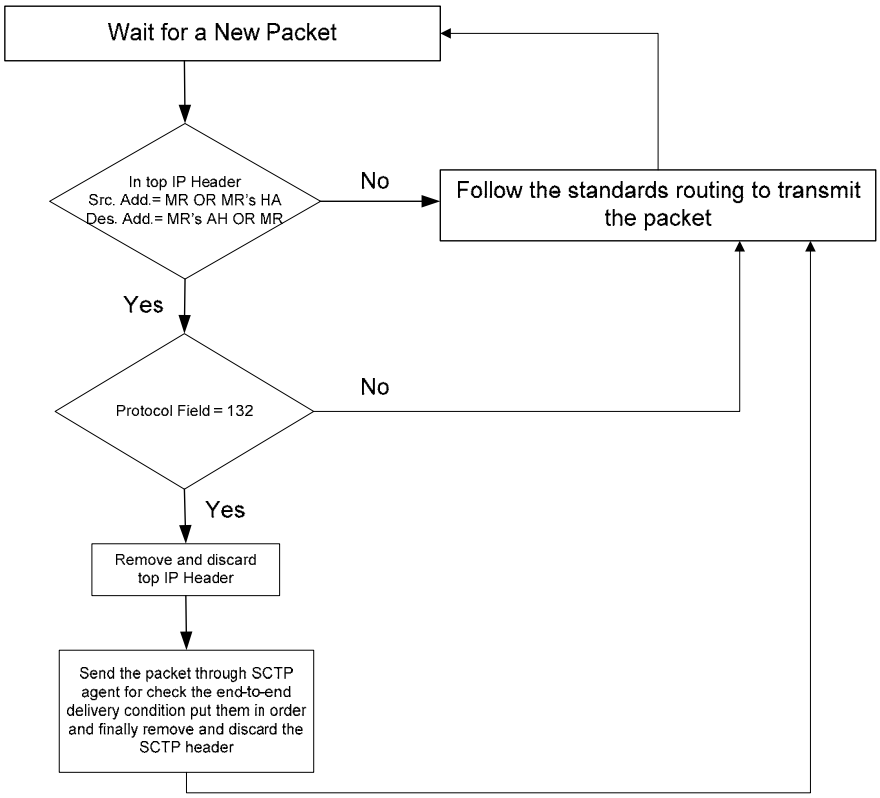

Figure 4-4: SCTP/IP decapsulation mechanisms for ongoing flow in nSCTP structure

4.4. nSCTP Protocol

Figure 4-5 shows the overall nSCTP mechanisms when a moving network changes its location and performs handover. The signal strength in wireless communications have two important thresholds; at below a specific threshold (Cx Thresh) the received signal level is weak and not recognisable, and above the other threshold (Rx Thresh) the signal strength is powerful enough for data transmission. In the area between Rx and Cx thresholds, the signal is partly detectable and can be used for some signalling messages like route advertisement but it is not strong enough for data transmission. As shown in Figure 4-5, a three-zone can be observed, namely: steady state, detecting and soft handover zones. In the steady state zone the MR is connected through one of its interfaces and in a stable condition communicates to the BS. In the detecting zone, another wireless access network is detectable and in the soft handover zone, which is the overlap area of two or more adjacent cells, is the region for obtaining the new IP address, adding it in to the SCTP association and finally, changes the primary path and sends the binding updates to the home agent. When MR moves into a neighboring coverage area or gets in to the soft handover zone, the signal strengths for both BSs are equal or greater than the Rx threshold value. The MR then attempts to get an IP address with the help of DHCP, SIP or any other methods. In the soft handover zone both MR's interfaces have their own IP addresses and they have been added to the SCTP association between the MR and MR-HA. This zone is the appropriate place for changing the primary IP address but the suitable time for performing this transaction is a challenging issue.

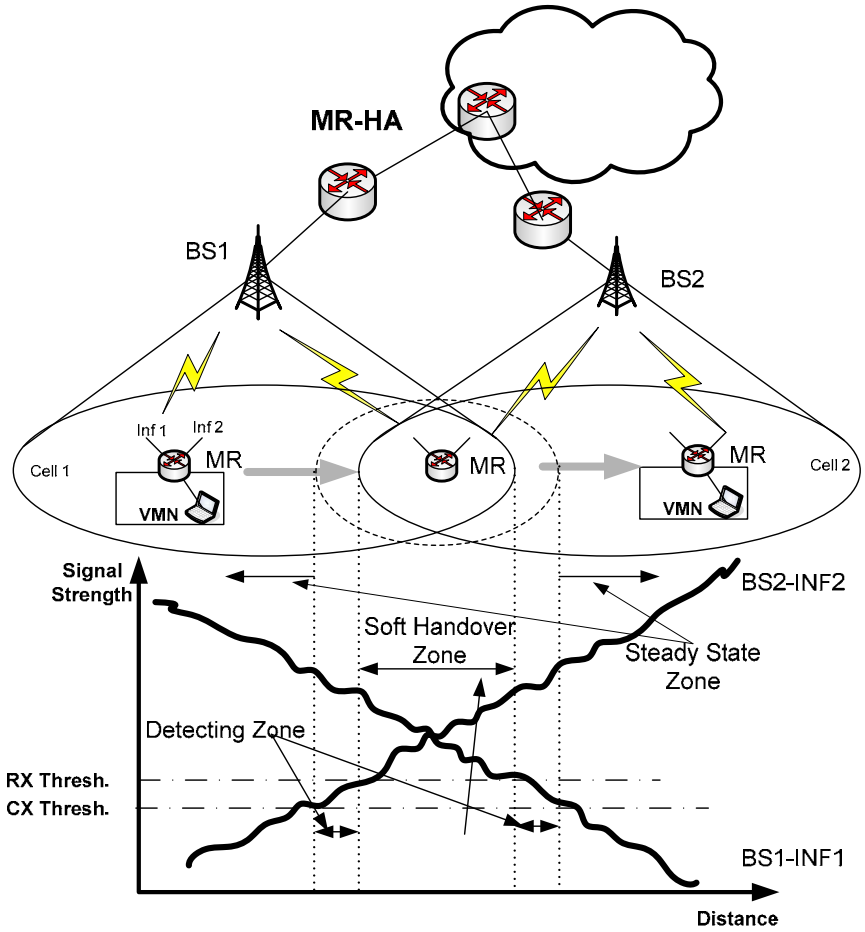

Figure 4-5: nSCTP handover management by the effect of signal strength thresholds

As SCTP is an end-to-end transport layer protocol, for providing seamless handover based on SCTP more than one interface at the mobile end is necessary. Also, software incompatibility caused by some applications that use TCP as a common reliable transport layer protocol. For avoiding these limitations and also to use the multi-homing feature of SCTP to improve the handover parameters, having another end-to-end connection between MR and MR-HA is proposed. In NEMO basic protocol, an IP-in-IP tunnel between these two entities (MR and MR's HA) is available. Upgrading this tunnel to support transport layer tunnelling (described in section 4.3) can facilitate the soft and seamless handovers in a NEMO scenario. Figure 4-6 depicts the moving network scenario with two data paths which is a common scenario for two independent wireless access technologies. The paths with label 1 and 3 are end to end that run transport layer protocols and the path with label 2 is IP-in-IP tunnelled.

Throughout path 3 which is the wireless part of heterogeneous wireless access technologies, multi-homing feature of SCTP has been used. Therefore, two paths via WLAN and UMTS can be observed; the path from WLAN-AP chosen as a primary for handling the traffic and the other path via UMTS node-B is chosen as an alternative path that can be changed to primary in the case of handover or instability in the path via AP.

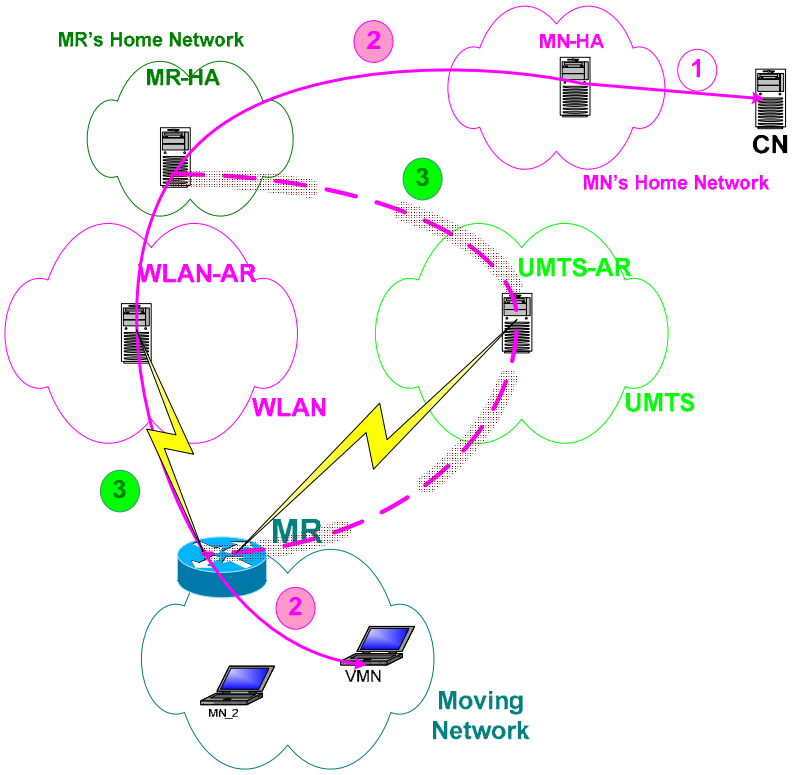

Figure 4-6: SCTP/IP encapsulation mechanisms for ongoing flow under nSCTP structure

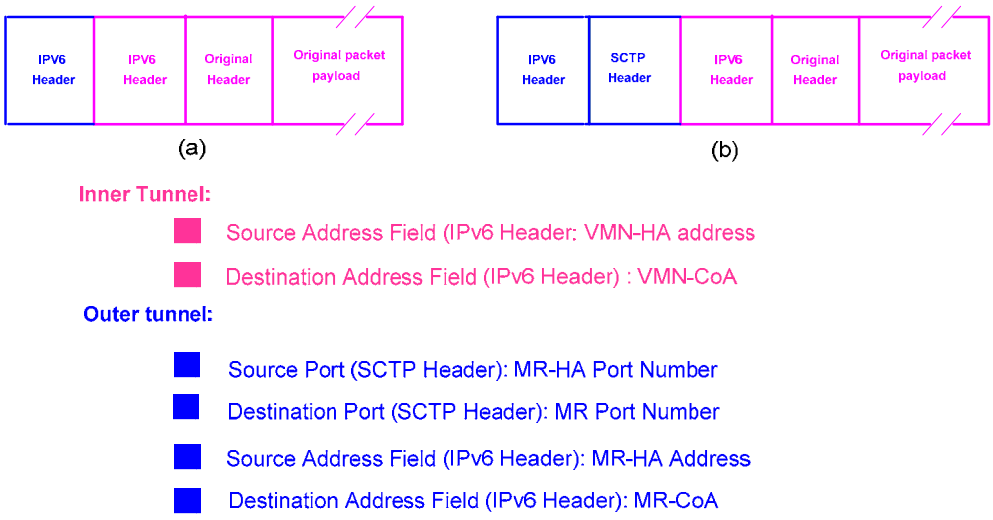

Figure 4-7: Packet format (a) In NEMO (b) In nSCTP

Figure 4-7(a) shows the packet configuration in the NEMO scenario which has changed to Figure 4-7(b) in the nSCTP configuration after deploying SCTP tunnelling header for the packet. The algorithms for the overall nSCTP mechanism for on-going flow during communication have been provided in the section 4.3. Encapsulation and de-encapsulation process should be done in MR and MR's HA that are supporting multilayer processing. The incoming packets which are destined to the other part of the network should be sent to the next hop without changing. This has been shown in the provided algorithms in Figure 4-2 and Figure 4-4.

4.5. Data and signalling paths in NEMO

In this section the signalling sequences involved in NEMO is summarised and it will compare with signalling time line in nSCTP in the next section.

Taking into consideration the moving network architecture (Figure 3-2) and the IP-in-IP encapsulation for Visiting Mobile Node (VMN – see Figure 4-6 and Figure 4-7), the whole data-packet paths in the order of occurrence are summarised in Figure 4-8:

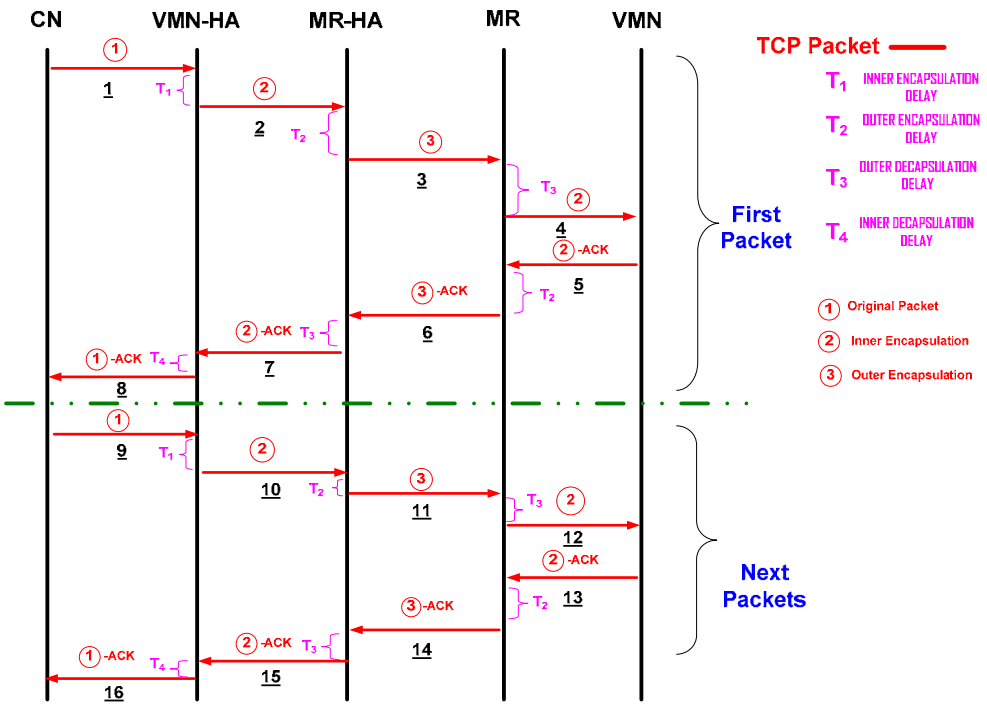

Figure 4-8: Data and signalling paths in NEMO structure

1. The packet should be sent to the VMN's home network by CN to fulfil NEMO requirements [42].

2. If the user uses a VMN, the packet is encapsulated for the VMN and is sent to the VMN via the MR's home network. The encapsulation delay is T_1. The tunnel entry point is the IP address of the user's HA, the tunnel end point is the VMN's CoA.

3. At the MR's HA, the packet is encapsulated again and sent to the MR's CoA. The tunnel entry point is the IP address of the MR's HA, the tunnel end point is the MR's CoA. The encapsulation delay is T_2.

4. When the MR receives the packet, it decapsulates the packet, strips off the outer tunnel, and sends it to the destination node, VMN. The decapsulation delay is T_3.

    a. The destination node decapsulates the packets again, removes the inner tunnel and retrieves the original data. The decapsulation delay is T_4.

5. The VMN sends a TCP acknowledgement to the source, acknowledging the receipt of the packet with the VMN and CN addresses for source and destination address fields respectively. This acknowledgement should be

tunnelled at the VMN with VMN-CoA and CN's in IP header fields with the encapsulation delay of T_1.

6. The MR relays the TCP acknowledgement to the MR's HA in an IP tunnelling. The encapsulation delay is T_2.
7. The MR's HA decapsulates the TCP acknowledgement in T_3 seconds and sends it to the user's HA.
8. The user's HA after decapsulation in T_4 time, relays the TCP acknowledgement to the Source acknowledging receipt of the packet.
    a. On receiving the TCP acknowledgement for the first packet, the Source increases the congestion window and sends a number of packets in the next transmission, dependent on the congestion window size (usually two packets)..
9. A group of packets is sent to the VMN's HA.
10. -16. The same procedure is repeated for the group of packets.

4.6. Data and signalling paths in nSCTP

One of the most important features of reliable transport layer protocols is their end-to-end communications, which is preferred to maintain in any practical solution for multi-homing in NEMO concept. In order to maintain this end-to-end communications, in nSCTP structure a transport layer protocol (e.g. TCP, SCTP or UDP) runs at two ends between the CN to the destination (e.g. VMN) and multi-homed SCTP is applied between the MR-HA and the MR. This can be achieved by enhancing the outer tunnel between the MR-HA and the MR to run SCTP between these two entities. In order to do so, an SCTP session should first be established between these two entities by using a 4-way handshake. Once the session is established communication can be started and as the MR detects a new AR on the other interface and gets the IP address, it will be added to the association by using Add-IP via ASCONF and ASCONF-ACK chunks. The new established path uses as an alternative path for the primary link. The relevant signalling and data transmission in nSCTP is illustrated in Figure 4-9.

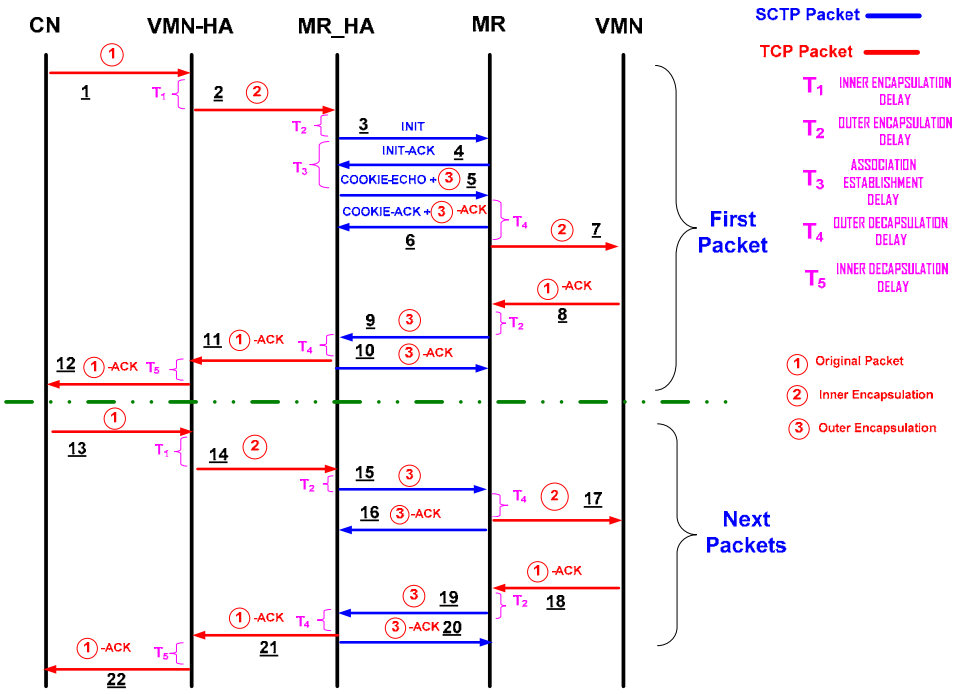

Figure 4-9: Data and signalling paths in nSCTP structure

1. The packet should first be sent to the VMN's home network by CN in the Figure 4-6 to fulfil NEMO requirements [42].
2. If the user uses a VMN, the packet is encapsulated for the VMN and is sent to the VMN via the MR's home network. The encapsulation delay is T1.
    a. At the MR's HA, the packet is encapsulated again and sent to the MR's CoA. The tunnel entry point is the IP address of the MR's HA, the tunnel end point is the MR's CoA. The encapsulation delay is T2.
3. The MR's HA sends an INIT message to the MR to initiate an association between two nodes.
4. The MR sends an acknowledgement to the MR's HA. The association establishment is T_3.
5. The MR's HA sends a Cookie Echo message to the MR. At the same time; it can start sending packets to the MR using data chunks in the Cookie Echo message.

6. The MR sends a Cookie ACK and a received-data acknowledgment to the MR's HA.
7. When the MR receives the packet, it decapsulates the packet, strips off the outer tunnel, and sends it over to the destination node, VMN. The decapsulation delay is T_4.
    a. The destination node decapsulates the packets again and retrieves the original data. The decapsulation delay is T_5.
8. The VMN sends a TCP acknowledgement to the source acknowledging the receipt of the packet. This acknowledgement is first sent to the MR.
9. The MR encapsulates the acknowledgment in T_2 seconds and transfers to the MR's HA.
10. The above SCTP acknowledgement is acknowledged by sending an SCTP acknowledgement from the MR's HA to the MR.
11. The MR's HA decapsulates the received acknowledgement in T_4 seconds and transfers the extracted TCP acknowledgement to the VMN's HA.
12. The VMN's HA after another decapsulation in T_5 seconds, relays the TCP acknowledgement to the CN and acknowledging the receipt of the packet.
    a. On receipt of TCP acknowledgement for the first packet, the Source increases the congestion window size and sends a number of packets (usually two).
13. The group of packets the Source now sends to the user's HA, depends on the congestion window size (usually two packets).
14. Packets get encapsulated for the VMN and are sent to the VMN via the MR's home network. The encapsulation delay is T_1. The tunnel entry point is the IP address of the user's HA, the tunnel end point is the VMN's CoA.
15. At the MR's HA, packets are encapsulated in the SCTP packets and sent to the MR's CoA. The tunnel entry point is the IP address of the MR's HA, the tunnel end point is the MR's CoA. The encapsulation delay is T_2.

a. At this stage, there are no INIT and INIT ACK messages, as the SCTP association is already established. Therefore, the association establishment time T_3=0.

16. The MR sends an SCTP acknowledgment to the MR'S HA confirming the receipt of the packets.

17. to 22. The same procedure of steps 7-12 is repeated for the group of packets respectively.

4.7. Enhanced MR and the MR's Home Network

As previously mentioned, in order for moving networks to benefit from multi-homing, an SCTP association should be established between the MR and the MR's HA. Consequently, the MR and the MR's HA should be enhanced to intercept SCTP packets. Figure 4-10 illustrates the encapsulation and de-encapsulation process that should take place in the MR and the MR's HA.

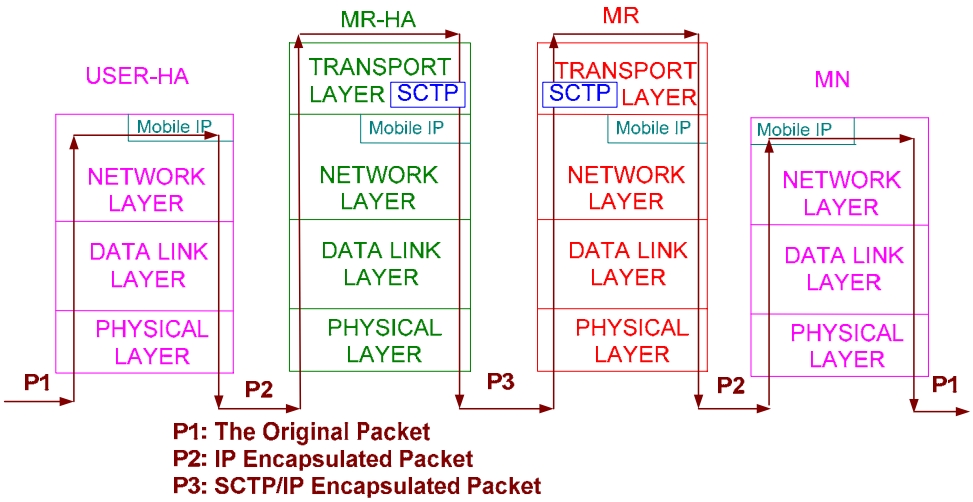

Figure 4-10: Enhanced encapsulation for the MR and the MR's HA

The user's HA encapsulates packets which are destined to mobile network, at the network layer and sends them to the MR's HA. The MR's HA encapsulates packets again at the network layer and sends them one layer up to the transport layer, where packets are encapsulated again with an SCTP header and then the

MR's HA sends packets to the MR. The MR decapsulates packets at the network layer and sends them up one layer to the transport layer, where the SCTP header is stripped off. Packets are then sent to the VMNs. In order for the MR and the MR's HA to create tunnels at the transport layer, these routers must have the ability of supporting multi-layer protocols.

4.8. Chapter Summary

After introducing the main problem of NEMO basic support protocol in vertical handovers in Chapter 3, a solution based on multi-homing in NEMO is presented in this chapter. Possible multi-homing configuration and the important criteria were studied and the most suitable configuration consisting of single MR, single HA and single MNP (1,1,1) was chosen as the most suitable option for moving network as it provides ubiquitous access, load sharing and reliability while taking advantage of less complexity in comparison with the other configurations. To enable (1,1,1) configuration on moving network, nSCTP, was presented as the new protocol that uses multi-homing feature of SCTP. Transport layer tunnelling was introduced in this chapter that will be replaced with outer IP-in-IP tunnelling in the original NEMO protocol and runs SCTP/IP encapsulator and de-encapsulator between MR and the MR-HA.

Details of the performing tunnels, data and signalling paths were taken into consideration in this chapter. nSCTP apart from solving the disruption in vertical handovers for moving network, benefits from keeping the end-to-end communication between sender and receiver. Also running another reliable transport protocol at the wireless hop(s) of the network can solve the random error-rate cased by the unreliable nature of wireless media locally without involving the sender and receiver nodes.

Efficiency of this protocol must be taken into consideration as transport layer tunnels involve some processing and bandwidth overhead on the system. In the next chapter performance analysis of TCP over nSCTP connection will be studied and the mathematical model will be presented.

Chapter 5. Performance analysis of TCP over nSCTP

TCP is the most used transport protocol and carries about 90 percent of Internet traffic [55] that requires reliability. TCP has originally been designed and optimised to work on wired network environments and its congestion control mechanisms cannot be adapted easily for wireless networks. TCP considers all the packet losses as the consequence of congestion in the network and therefore reduces the congestion window follow up with each detected loss. This reduction can dramatically reduce the performance of TCP in a pure wireless connection or a combination of wired and wireless network, while the significance of losses are due to the nature of wireless medium. This problem can be even worse and more serious when the nodes are mobile and involved in handover, which often result in disconnectivity or connection disruption.

Some newly developed mobility management protocols that solve the connection disruption during the handover period, use the multi-homing feature of SCTP such as Mobile SCTP (mSCTP) [20, 21 2005] and Cellular SCTP (cSCTP) [56] (explained in section 2.5) . These protocols apply SCTP multi-homing [3] and Dynamic Address Reconfiguration (DAR) extension [7] in order to provide a soft and seamless vertical handover for individual mobile nodes. In the previous chapter nSCTP that uses the multi-homing feature of SCTP to facilitate the seamless handover for moving network in a heterogeneous environment has been proposed.

In nSCTP, SCTP tunnel is applied between the mobile router (MR) and its home agent (MR's HA). These two routers are multi-interfaced routers with capability of supporting transport layer tunnelling based on SCTP/IP encapsulation/de-encapsulation algorithms proposed in sections 4.3.2 and 4.3.4. In this Chapter performance of nSCTP is evaluated. TCP and SCTP analytical models are presented and subsequently nSCTP as a function of TCP is analysed. Also the impact of applying transport level tunnels based on this model is studied. In addition the essential QoS parameters such as handover delay, end-to-end

throughput and packet loss are compared in original NEMO structure and the new proposed protocol. And finally, the models have been evaluated by numerical applications and discussion of the result.

5.1. Transport Layer Tunnelling Overview

The transport layer tunnelling as described in the previous Chapter is a method for building a virtual circuit, by aggregating flows between two nodes or routers and treating them like a single connection. This tunnelling has been widely used in different applications such as SSH[46], VTun[47] and HTun[48, 57] and in this Thesis nSCTP was proposed to smooth the handover based on transport layer tunnelling.

To answer the question "is it a good idea to encapsulate on transport layer protocols?" the advantages and disadvantages of transport layer tunnels are presented in the next section.

5.1.1. Advantages of transport layer tunnelling

Transport layer tunnelling benefited in different criteria which are summarised as follow:

- By using reliable transport layer protocol tunnelling (e.g. TCP or SCTP), the fairness among aggregated flow can be improved and several protocols can share a pre-defined tunnel and transparently send the segments through that. UDP traffic is not TCP and/or SCTP traffic friendly and as Floyd et al. mentioned in [50] UDP is an unresponsive protocol that does not use end-to-end congestion control and does not reduce its load on the network when subjected to packet drops.
- The tunnel can reduce the overall amount of traffic sent. The amount of retransmission per connection is reduced by over 500% [58] as the tunnel provides reliability in the highly congested part of the network.
- Tunnel can guarantee the minimum bandwidth[59] as at least some number of bytes of data over a period of a time is transmitted.

- Tunnel can share the possible bandwidth between all users of tunnel in a fair way. Define the QoS policies on the tunnel is more realistic as the entire transmitted packets will be under control.
- In sequence forwarding which is the natural effect of the packets' encapsulation.
- Reducing the number of flow on the routers inside the tunnel.

5.1.2. Drawbacks of transport layer tunnelling

In spite of all the benefits of transport layer tunnelling it suffers from some well-known weaknesses:

- Adding another reliable transport protocol in the middle of an end-to-end connection employs more management complexity as well as additional routers' modules which should be provided on ingress and egress routers.
- The TCP timeout policies work fine in the wired infrastructure networks where it is assumed that all packet losses are because of the congestion in the network. This scenario does not work very well in the wired-cum-wireless environment as the connections are involved in a higher percentage of packet loss in the air interface. TCP assumes that all losses belong to the network congestion and reduces the transmission window which has resulted in reduction of end-to-end throughput. Stacking one reliable transport protocol on another in a connection as they could have different speeds and latency, in some wired networks' scenarios means the performance can be dramatically reduced. This probably is not the case when the tunnel is going to be set on the wireless part of the network as almost all the packet losses are retransmitted in the outer tunnel and will contribute more in increasing the performance of the connection.
- The Transport tunnels degrade the RTT as new encapsulation and decapsulation should be made. Based on the experimental analysis by Lee et.al. in [58] degrading of 280% is estimated.

5.2. Handover Delay investigation in nSCTP and NEMO

Handover delay is defined as the period of time between the moment which an existing IP address becomes unreachable for an end-to-end transmission and the time a new IP address is allocated to the MR and the transmission being resumed.

5.2.1. Handover Delay in NEMO

As presented in section 3.3 and specified in RFC 3344 [1] different parameters are involved in handover latency:

- Agent discovery time (T_{ad}) consists of a solicitation message (T_{sol}), an advertisement message (T_{adv}) and a CoA processing time (T_{CoA}). Therefore:

$$T_{ad\text{-}NEMO} = T_{sol} + T_{adv} + T_{CoA} \qquad (5\text{-}1)$$

- At this stage, the MR's interface has a new CoA, which should be registered with its home network, where packets can be diverted to the new location. Agent registration time (T_{reg}) consists of sending a request message to the MR's HA (T_{REQ}), binding the new CoA inside the home agent (T_{BU}) and finally sending back confirmation to the MR (T_{ACK}). Therefore:

$$T_{reg\text{-}NEMO} = T_{REQ} + T_{BU} + T_{ACK} \qquad (5\text{-}2)$$

From equations (5-1) and (5-2) , the total handover delay in NEMO is:

$$T_{NEMO} = T_{ad\text{-}NEMO} + T_{reg\text{-}NEMO} = T_{sol} + T_{adv} + T_{CoA} + T_{REQ} + T_{BU} + T_{ACK} \qquad (5\text{-}3)$$

5.2.2. Handover Delay in nSCTP

When the mobile router enters into the soft handover zone (Figure 4-5), the second interface of the MR goes through the same process as mentioned in the previous section to get a new CoA. Therefore; the agent discovery time remains unchanged:

$$T_{ad\text{-}nSCTP} = T_{sol} + T_{adv} + T_{CoA} \quad (5\text{-}4)$$

The obtained IP address on the unallocated interface of MR should be registered with nSCTP ($T_{reg\text{-}nSCTP}$) and then set the new IP as primary IP address. The time for adding IP and changing primary address as discussed in section 2.5.2, consists of an ASCONF message (T_{ASConf}) and the confirmation acknowledgement ($T_{ASConf\text{-}ACK}$). Therefore:

$$T_{reg\text{-}nSCTP} = 2 \times (T_{ASConf} + T_{ASConf\text{-}ACK}) \quad (5\text{-}5)$$

From equations (5-4) and (5-5), the total handover delay in nSCTP is:

$$T_{nSCTP} = T_{ad\text{-}nSCTP} + T_{reg\text{-}nSCTP} = T_{sol} + T_{adv} + T_{CoA} + 2 \times (T_{ASConf} + T_{ASConf\text{-}ACK}) \quad (5\text{-}6)$$

5.3. End-to-End Throughput Investigation in nSCTP and NEMO

In any data transmission system, one of the most important parameters from the user's point of view is the amount of data transmission during a certain time, which is identified as end-to-end throughput. Some parameters like signalling overhead, which in the case of NEMO is caused by double tunnelling and possible disconnectivity during the handover, can dramatically reduce the throughput. On the other hand, upgrading the outer tunnel to deploy SCTP multi-homing in the case of nSCTP creates another undesirable overhead. In this section, the reduction of throughput caused by handovers and tunnels are calculated.

Throughput is defined as the number of successful bits transferred in a certain period of time and also TCP data transmission is the baseline of this calculation. Therefore:

$$Throughput(bps) = \frac{BitsTransfered(b)}{Time(s)} = \frac{\mu}{T_s} = \eta \quad (5\text{-}7)$$

Analytical calculation of SCTP throughput is presented in several papers. Fu et al. [60] presented a multi-homed SCTP analytical model with the support of simulation. In a similar work [61] has developed a new analytical model to study the SCTP throughput performance in an integrated WLAN/cellular networks. In

all these works, the performance analysis for a single mobile node is evaluated. In this section, the performance of the newly proposed protocol (nSCTP) in a group mobility handover is presented and the result has been compared with the NEMO basic support protocol.

5.3.1. End-to-End Throughput in nSCTP and NEMO

The NEMO basic support protocol [2] consists of two tunnels that inject some bits of overhead, which results in throughput reduction as shown in the following equation:

$$\eta_{NEMO} = \frac{\mu - (\sum_{i=1}^{\delta} D_{NEMO}(i) + l_{IPT-inner} + l_{IPT-outer})}{T_s} \tag{5-8}$$

Where $l_{IPT-inner}$ and $l_{IPT-outer}$ are the bits overhead for the inner and outer tunnelling overhead in NEMO architecture respectively. D_{NEMO} represents bits losses during the handover caused by delay in the case of having δ handovers. η is the throughput of the system within time T_s . On the other hand;

$$\sum_{i=1}^{\delta} D_{NEMO}(i) = \delta \times \overline{D_{NEMO}} \tag{5-9}$$

Where, $\overline{D_{NEMO}}$ is the average bits lost in each handover, hence:

$$\eta_{NEMO}(bps) = \frac{\mu - (\delta \times \overline{D_{NEMO}} + l_{IPT-inner} + l_{IPT-outer})}{T_s} \tag{5-10}$$

Suppose that the average NEMO handover delay is T_{NEMO} then, the average amount of data loss based on the TCP load for end-to-end connection is:

$$\overline{D_{NEMO}} = \mu \times \frac{\overline{T_{NEMO}}}{T_s} \tag{5-11}$$

In all cases for a visiting mobile node joined in a moving network, the inner tunnelling exists. Then:

$$l_{IPT-inner} = \mu \times \frac{F_{MIP}}{P_{MTU}} \tag{5-12}$$

Where the P_{MTU}, which is the Maximum Transmission Unit (MTU) refers to the size of largest packet that can be transferred in one frame over a network, is assumed to be 1500 bytes (in Ethernet) and the IPv6 header is 40 bytes (F_{MIP}):

$$l_{IPT-inner} = 0.02\dot{6} \times \mu \tag{5-13}$$

The outer tunnelling will happen only when the MR is out of its Home Agent area. Therefore:

$$l_{IPT-outer} = \mu \times \frac{T_{Fl}}{T_S} \times \frac{F_{MIP}}{P_{MTU}} \tag{5-14}$$

Then,

$$l_{IPT-outer} = 0.02\dot{6} \times \frac{\mu}{T_S} \times T_{Fl} \tag{5-15}$$

Where, T_{Fl} is the time that MR stays in a foreign network. By inserting equations (5-11), (5-13) and (5-15) into equation (5-10):

$$\eta_{NEMO} = \frac{\mu}{T_s} - \frac{\mu}{T_s^2}[(\delta \times \overline{T_{NEMO}}) + 0.02\dot{6}(T_s + T_{Fl})] \tag{5-16}$$

As shown in the above formula the end-to-end throughput of NEMO is decreased directly by increasing the number of handovers. The inner and outer tunnels reduce the overall throughput constantly by imposing a fixed amount of overhead per MTU.

5.3.2. End-to-End Throughput in nSCTP

Applying changes in the NEMO solution to achieve the nSCTP structure, makes some unpredictable changes to the end-to-end throughput. On one side, reducing the handover latency in nSCTP to about zero (discussion on section 4.4) can guarantee more data transmission and on the other side increasing the size of the outer tunnel should be applied to all packets, injecting additional signalling overhead on the network. The following calculations are based on the reduction of the throughput caused by handover and tunnelling. Similarly to the previous section the baseline for this reduction is the throughput regardless of tunnels and handovers.

The nSCTP structure consists of two tunnels and δ handovers that impose some overhead as shown in the following equation:

$$\eta_{nSCTP}(bps) = \frac{\mu - (l_{IPT-inner} + l_{nSCTPT-outer} + \sum_{i=1}^{\delta}(T_{nSCTP}(i) + l_{DAR}))}{T_s} \quad (5\text{-}17)$$

Where, η_{nSCTP} represents the throughput for nSCTP and μ is the total bits without having the tunnels and handovers.

L_{DAR} is the required signalling for performing a handover and T_{nSCTP} is the handover delay and will be explained in section 5.5:

$$\overline{T_{nSCTP}} \approx 0$$

The signalling (l_{DAR}) consists of three sets of chunks each including a control chunk and its acknowledgment used in the purpose of add-IP, set primary link and delete IP as described in section 2.5.2. These chunks consist of an ASCONF message (T_{ASConf}) and the confirmation acknowledgement ($T_{ASConf\text{-}ACK}$) and can be modelled as:

$$l_{DAR} = 3(C_{ASConf} + C_{ASConf-ACK}) \quad (5\text{-}18)$$
$$= 3 \times (256 + 64) = 960 bits \quad \text{(for IPv4)}$$

$$l_{DAR} = 3(C_{ASConf} + C_{ASConf-ACK}) \quad (5\text{-}19)$$
$$= 3 \times (448 + 64) = 1536 bits \quad \text{(for IPv6)}$$

In equation (5-17), $l_{IPT-inner}$ and $l_{nSCTPT-outer}$ are the effect of inner IP tunnelling and the outer nSCTP tunnelling respectively. That can be formulated as:

$$l_{IPT-inner} = \mu \times \frac{F_{MIP}}{P_{MTU}} = \mu \times \frac{40}{1500} = 0.026\dot{\mu} \quad (5\text{-}20)$$

F_{MIP} is the size of outer tunnelling and is equal to the size of IPv6 header attached to the tunnelled packets. P_{MTU} is a standard MTU for each packet. The outer tunnel is a combination of IP and SCTP headers which are:

$$l_{nSCTPT-outer} = \mu \times \frac{F_{MIP} + F_{SCTP}}{P_{MTU}} = \mu \times \frac{40+16}{1500} = 0.037\mu \quad (5\text{-}21)$$

Where, F_{MIP} and F_{SCTP} represents the bit overhead for IP and SCTP respectively, the SCTP header for a packet is 16 bytes which consists of 12 bytes SCTP common header and needs at least one chunk with 4 bytes header as described in RFC2960 [3].

As all the calculations are based on IPv6 therefore from the equations (5-17), (5-19), (5-20) and (5-21) throughput for nSCTP will be:

$$\eta_{nSCTP}(bps) = \frac{\mu - 0.026\mu - 0.037\mu - \delta \times 1536}{T_s} = \frac{0.9364\mu - 1536 \times \delta}{T_s} \quad (5\text{-}22)$$

5.4. Packet Loss Investigation in nSCTP and NEMO

5.4.1. Packet loss in NEMO (L_{NEMO})

Packet loss, which is one of the major parameters in any handover scenario, is the total number of packets lost during the handover period. This parameter directly depends on the period of time that the MR is inaccessible, caused by handover. Packet loss of NEMO handover can be represented as follows:

$$L_{NEMO} = \sum_{i=1}^{\delta} \frac{l_{NEMO}(i)}{P_{MTU}} = \frac{\delta \times l_{NEMO}}{P_{MTU}} = \frac{\delta \times \frac{\mu_{TCP}}{T_s} \times \overline{T_{NEMO}}}{P_{MTU}} = \delta \times \overline{T_{NEMO}} \times \frac{\mu_{TCP}}{T_s \times P_{MTU}} \quad (5\text{-}23)$$

In the above equation, P_{MTU} is the size of each packet, l_{NEMO} is the bits data loss caused by NEMO handover with the average handover delay $\overline{T_{NEMO}}$ during the total time of system running T_s and with δ handovers.

5.4.2. Packet loss in nSCTP (L_{nSCTP})

Similar to analysis presented in section 5.4.1, packet loss for nSCTP can be calculated as:

$$L_{nSCTP} = \sum_{i=1}^{\delta} \frac{l_{nSCTP}(i)}{P_{MTU}} \approx \frac{\delta \times l_{nSCTP}}{P_{MTU}} = \frac{\delta \times \frac{\mu_{TCP}}{T_s} \times \overline{T_{nSCTP}}}{P_{MTU}} = \delta \times \overline{T_{nSCTP}} \times \frac{\mu_{TCP}}{T_s \times P_{MTU}} \quad (5\text{-}24)$$

Where, P_{MTU} is the size of MTU, l_{nSCTP} is the data loss, $\overline{T_{nSCTP}}$ the average time of nSCTP handover delay, T_s running time and δ the number of handover.

5.5. Comparison of analytical results in NEMO and nSCTP

In sections 5.2 to 5.4 analysis of handover parameters in two different solutions for group mobility handover, NEMO and nSCTP are presented. In this section, comparisons between these two schemes for handover latency, throughput and packet loss are provided.

5.5.1. Handover Latency Comparison

The handover delays for NEMO and nSCTP have been formulated in the equations (5-3) and (5-6) respectively. The comparison of these results shows that agent discovery time will be the same in both cases and depends on the solicitation message, advertisement message and allocation of CoA parameters (equations (5-1) and (5-4)). Using multi-interface MR and enabling the multi-homing feature of nSCTP causes these signalling and processing delays that needs to be completed at the overlap area while another interface is still in communication through the old wireless access network. Therefore:

$$T_{ad-nSCTP} \approx 0 \text{ or } T_{ad-NEMO} \gg T_{ad-nSCTP} \quad (5\text{-}25)$$

In the same manner,

$$T_{reg-nSCTP} \approx 0 \text{ or } T_{reg-NEMO} \gg T_{reg-nSCTP} \quad (5\text{-}26)$$

As $T_{NEMO} = T_{ad\text{-}NEMO} + T_{reg\text{-}NEMO}$ and $T_{nSCTP} = T_{ad\text{-}nSCTP} + T_{reg\text{-}nSCTP}$

Therefore,

$$T_{NEMO} \gg T_{nSCTP} \qquad (5\text{-}27)$$

5.5.2. Throughput Comparison

In sections 5.3.1 and 5.3.2 analysis of end-to-end throughput in two different solutions for group mobility handover, NEMO and nSCTP, are presented. In this section, the numerical results and the comparison between these two schemes are provided.

Based on equation (5-22), nSCTP has a direct effect on the throughput which reduces the overall throughput by approximately 6.36 percent (or coefficient of 0.9364) regardless of the handover rate. The handover in this scheme has little impact on the throughput (1536 bits per handover). In the NEMO scenario when there is no handover and the mobile router stays in its home network, which normally is not the case for mobile networks, no tunnelling overheads injected in the network. MIP and consequently NEMO put a huge impact on handover delay, which is defined as the period of time between the moment that an existing IP address becomes unreachable for an end-to-end transmission until the time a new IP address is allocated to the MR and the transmission is resumed. In NEMO, when a MR moves to the new coverage area, the packet cannot be diverted to the new location of the MR unless cell agent discovery procedures [1] for acquiring a new CoA and bind update procedure for registering this new CoA with MR-HA are performed. nSCTP treatment for handover is different as inside the soft handover zone, while the other interface is still in transmission, agent discovery procedure for acquiring CoA on the non-engaged interface and register this address in the SCTP association between MR and MR-HA can be done. Therefore, it is quite feasible to say that handover delay for NEMO is much greater than nSCTP ($T_{NEMO} \gg T_{nSCTP}$). The amount of handover delay for NEMO can significantly reduce the throughput of this protocol based on equation (5-16).

The result of numerical examples for comparison of the end-to-end throughput for both schemes is provided in Figure 5-1, while maximum 20 handovers are experienced during 500sec. In this experiment, throughput ratio (nSCTP:NEMO)

has been compared in different range of data rate within 4Kbps to 2Mbps. The outcome of this experiment depicts that in low data rate and low handover rate when the throughput ratio is less than "1", NEMO showing better performance and by increasing the data rate and particularly in high handover rate scenarios, up to 20 percent improvement can be observed with nSCTP.

The results show that in the low handover rate NEMO has better response compared to nSCTP but it drops significantly by increasing the handover rate. Based on this numerical example (shown in Figure 5-1), nSCTP employed initial overhead on the packets, therefore, a deduction in throughput compare to NEMO can be observed at the low or non-handover rate scenarios.

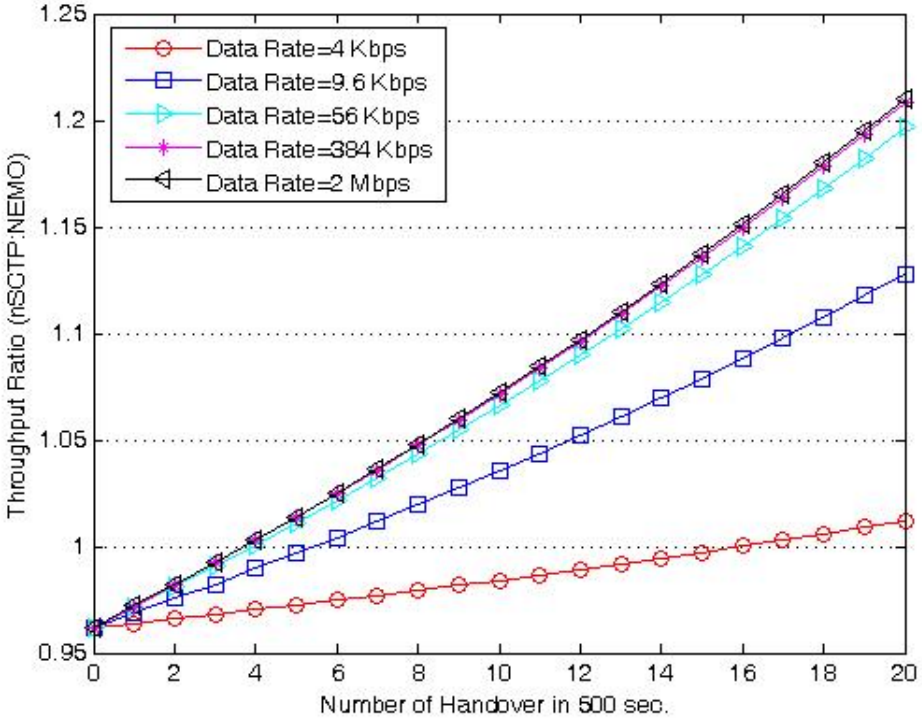

Figure 5-1: Throughput comparisons while the transmission rate changes

5.5.3. Packet Losses Comparison

In sections 5.4.1 and 5.4.2 the impact of NEMO and nSCTP on packet losses has been modelled. The calculation results for these protocols (equations (5-23) and (5-24)) show that packet losses are directly dependent on the handover latency and the number of handovers in both cases. As proved earlier in section 5.5.1 this

delay in the case of nSCTP is much less than NEMO (equation (5-27)) which will result in a smaller number of packet loss in nSCTP compare to NEMO or:

$$L_{NEMO} \gg L_{nSCTP} \tag{5-28}$$

5.6. TCP Model

A simple model of TCP that consists of slow start and congestion avoidance has been considered in this section. For simplification, fast retransmission and fast recovery have not been taken into the consideration. The presented model is based on the Reno version of TCP, as described in [62] and the throughput model presented in [63]. In this model, steady state throughput of a bulk TCP flow transfer in an end-to-end connection has been assumed. TCP's congestion control window size is denoted by W, is increased by 1/b for each received acknowledgment.

RTT_{TCP} is defined as a measure of the time it takes for a TCP segment to travel from a source to destination and receive the Ack with the assumption that processing time is negligible compared to RTT_{TCP}. Also packet loss can be detected by either three consecutive acknowledgments (T_d) or time out (T_o) with the loss rate of p in an end-to-end connection. In addition, assuming that packet losses are correlated among the back-to-back transmissions within a round so if a packet is lost, all remaining packets transmitted until the end of that round are lost, Equation (5-29) shows the steady state TCP throughput [63]:

$$T_{TCP} = \min\left(\frac{W_{\max}}{RTT_{TCP}}, \frac{1}{RTT_{TCP}\sqrt{\frac{2bp}{3}} + T_O \min\left(1, 3\sqrt{\frac{3bp}{8}}\right) p\left(1+32p^2\right)}\right) \tag{5-29}$$

5.7. SCTP Model

Most of SCTP mechanisms for flow and congestion control are inherited from TCP. SCTP congestion control mechanism is similar to TCP Reno. The sender side applies timeout retransmission, fast retransmission and congestion avoidance. In [64] Yi et al., adapted the throughput of the TCP analytical model

(proposed by Padhye et al. [63]) for SCTP model when the multi-homing has not taken into consideration. In another work Basto et al. [65] adjusted the SCTP sender throughput with TCP model in [63].

To keep track of the models developed in [63-65] and compatibility with TCP model the same notations and expression as shown in Equation (5-29) can be applied for throughput in SCTP by replacing RTT_{TCP} with RTT_{SCTP}.

5.8. nSCTP Model

An end-to-end TCP connection is considered in this section. TCP has the most used transport protocol for carrying the reliable traffic in the current Internet infrastructure and mobile communication. Independent operation of TCP and SCTP has been considered in sections 5.6 and 5.7. Traffic to and from moving networks in a heterogeneous environment passes through different types of infrastructure media. In the wireless part of nSCTP topology, communications are involved in two major issues. Firstly, micro and macro mobility (intra-domain and inter-domain handover respectively) causes connection disruption and secondly, high signal to noise ratio caused by the nature of air interface. These two issues can dramatically reduce the performance of an end-to-end connection as term "p" in the Equation (5-29) is increasing.

In order to model the nSCTP, the controlling system of this protocol is used which is shown in Figure 5-2.

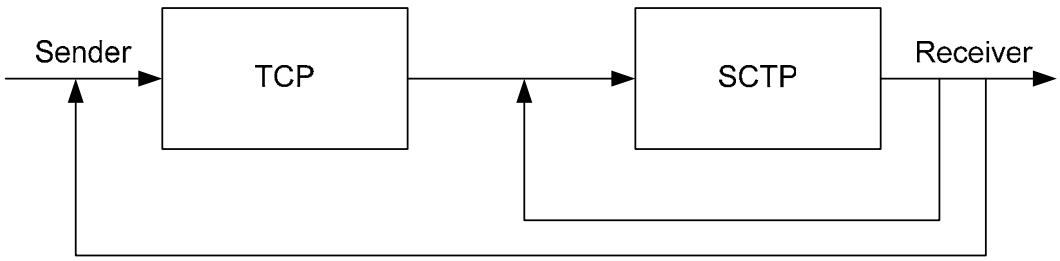

Figure 5-2: nSCTP block diagram structure

The principal of nSCTP is to keep the end-to-end communication for TCP and solve the wireless weaknesses of moving network structure locally. In this model it is assumed that the TCP segment size is smaller than the SCTP segment size and each TCP segment will be encapsulated inside a single SCTP segment and transmitted to the other end. This will simplify the model as the complex packet fragmentation process does not need to be addressed. SCTP module in the Figure 5-2 is responsible for error detection and retransmission between MR and its home agent MR-HA and TCP keeps track of the connection between the CN and the MN. Therefore as explained in Chapter 4 SCTP multi-homing can obtain the responsibility of the mobility and smoothing the handover (also presented in [8, 21 2005]).

In nSCTP model the RTT_{TCP} increases as SCTP module introduces a new latency in terms of segments processing, multi-homing failover mechanism and retransmission if needed. Segment processing delay compared to transmission delay that can form RTT_{SCTP} is negligible, and the multi-homing failover delay has been proved in section 5.5.1 to be almost zero. Retransmission applies some delay on the system which reduces the throughput of the whole system but on the other hand can enhance the overall performance as the lost packets can be retransmitted locally.

If it is supposed that the loss probability and round trip time in the SCTP part of network is $P_{Wireless}$ and RTT_{SCTP} respectively, then the throughput for this part can be calculated as Equation *(5-30)*

$$T_{Wireless} = \frac{1}{RTT_{SCTP}\sqrt{\frac{2bp_{wireless}}{3}} + T_{O-SCTP}\min\left(1,3\sqrt{\frac{3bp_{wireless}}{8}}\right)p_{wireless}\left(1+32p_{wireless}^{\ 2}\right)} \qquad (5\text{-}30)$$

For the end to end connection loss probability (p) is a sum of the loss probability in wired and wireless (P_{wired} and $P_{wireless}$ respectively) part of the network. Therefore,

$$p = p_{wired} + p_{wireless} - (p_{wired} \cdot p_{wireless}) \qquad (5\text{-}31)$$

As the value of probabilities in wired and wireless are relatively low and close to zero therefore,

$$p_{wired} \cdot p_{wireless} \approx 0 \tag{5-32}$$

Hence:

$$p \approx p_{wired} + p_{wireless} \tag{5-33}$$

Therefore, TCP throughput in the wired part of the network:

$$T_{Wired} = \frac{1}{RTT_{SCTP}\sqrt{\frac{2bp_{wire}}{3}} + T_{O-TCP}\min\left(1, 3\sqrt{\frac{3bp_{wire}}{8}}\right)p_{wire}\left(1+32{p_{wire}}^2\right)} \tag{5-34}$$

As shown in Figure 5-2, the wired and wireless modules of this control system are formed in a series combination. Therefore, the overall throughput for the whole system will be the minimum throughput of each subsystem. Also the achieved throughput for this section will consist of some tunnels' overheads due to the tunnels at IP and SCTP level that should be deducted from the result. Therefore:

$$T_{nSCTP} = \min(T_{Wireless}, T_{Wired}) \times (MTU - nSCTP_{Overheads}) \tag{5-35}$$

Where in the equation *(5-35)* $T_{Wireless}$ and T_{Wired} are the throughputs for wireless and wired subsystems and can be calculated by equations *(5-30)* and *(5-34)* respectively. MTU is the maximum size of transmitted packets and $nSCTP_{Overheads}$ is the amount of bit overheads applied on each packet that depend on the type of the network layer protocol (IPv4 or IPv6) and overheads on SCTP tunnels encapsulation explained in section 5.3.1.

5.9. Numerical result and discussions

The numerical result for throughput comparison between TCP and nSCTP are shown in Figure 5-3. In this result the total amount of packet loss has been assumed to be fixed within the entire end-to-end connection at 5 percent. The ratio of changes in the wired and wireless part of network is changed. The

cumulative acknowledgement ('b' in the throughput formulas) is assumed to be fixed at 2 and the size of RTT in the end to end connection is assumed to be double the size of RTT in the wireless part of the network. IPv4 is assumed to handle the network layer tunnels therefore the overheads as calculated in section 5.3.1 is set to 156 bits per packet.

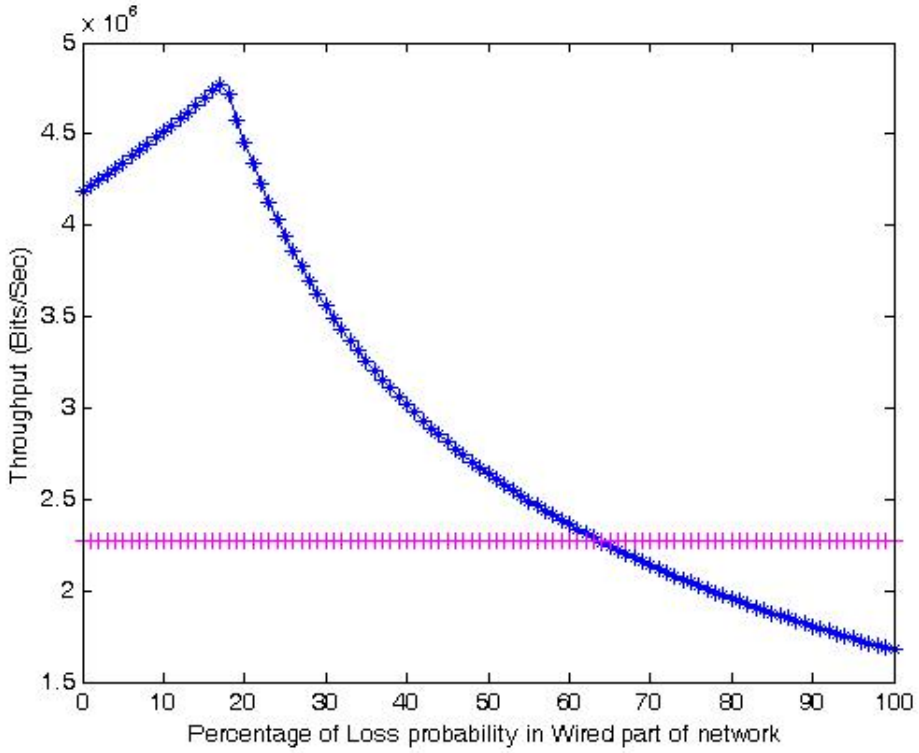

Figure 5-3: TCP Throughput in the case of NEMO and nSCTP while the ratio of loss changes in the wireless and wired part of the network

As it could be observed in Figure 5-3 while the loss percentage in the wire part of network is lower than in loss percentage in the wireless part of the network the throughput in the case of nSCTP is almost twice than NEMO. The result shows that from 5% overall packet loss the optimal behaviour can be achieved where about 20% of losses are on the wired connection and 80% are on the wireless connection. As the loss probabilities increases in the wired part of the network the performance of the nSCTP decreases and it will deteriorate where more than 85% of loss is caused on the wired connections.

In SCTP over TCP the result shows better performance compared to TCP as the packet losses can be handled locally with the lower RTT in the wireless hops. In about 80% of losses on the wireless link(s) the maximum throughput could be achieved. When the ratio of losses in the wired hops increases the throughput will be decreased as most of the errors need to be resolved between the sender and the receiver. When the majority of losses are on the wired sections (more than 65% in this example) the throughput of SCTP over TCP will be worse than TCP as some bits overhead are constantly applied to the network.

5.10. Chapter Summary

After proposing nSCTP based on the transport layer tunneling techniques presented in Chapter 4, the advantages and disadvantages of this protocol discussed in this Chapter. The new proposed protocol, smoothes the handover and eliminates connection disruption during vertical handover period in moving networks. However, nSCTP applies some signalling and processing overheads on the system. In order to study the level of improvement, three parameters including handover latency, throughput and packet loss were compared. The results show that handover latency is almost zero in nSCTP as the new connection will be set up before the old connection disconnects completely. As the handover latency has direct impact on the packet loss therefore in comparison to NEMO, the amount of packet loss in nSCTP is negligible. The throughput results show that in the case of small handover rate or when the mobile router is in the stationary position NEMO shows better response compare to nSCTP. While by increasing the number of handovers or the bit-rate of the system nSCTP shows better behaviour.

In the next stage the probability of the loss taken into consideration. nSCTP retransmits the packet loss inside the outer tunnel locally, without involving the corresponding nodes and the mobile node. This will improve the performance of the network as the loss packets are retransmitted within a smaller round trip time. TCP and SCTP slow start and congestion avoidance were considered in this analysis. The results show that, when the majority of packet losses occur inside

the wireless/mobile part of the network, the nSCTP demonstrates better performance while in the opposite condition the performance of NEMO takes advantage. However, it is not normally the case as most of the packet losses are due to the nature of wireless media.

Chapter 6. Simulation studies of the Performance of SCTP and nSCTP

In this chapter, the performance of handover at the transport level with SCTP is compared with handover using Mobile IP, the widely use network-layer mobility management handover solution. A three-phase simulation study is presented in this chapter. Firstly, for analysing the performance of SCTP, a 'basic' SCTP protocol without enabling its multi-homing feature is compared with three versions of TCP including Tahoe [66], NewReno [67] and SACK (Selective Ack) [68] in a combined wired and wireless topology.

Reliable transport layer protocols like TCP and SCTP used in usual wired networks do not perform properly in wireless scenarios. This is due to misinterpretation of lost packets as congestion, while they could be the result of high bit error-rate in the wireless channel, wireless interference or the mobility of the nodes. Although TCP was originally designed and optimized for wired networks, in order to enable seamless integration of cellular networks with the Internet, TCP seems to be an appropriate choice.

Most applications such as web browsing and FTP require reliable and in-order delivery of packet between two endpoints. TCP and SCTP are two transport layer protocols that build reliable and in-order delivery of data between two end hosts over an unreliable IP service. TCP and SCTP congestion Control is the ability of the sender to adjust the transmission rate based on the network's condition. the congestion control was first standardized in RFC2001[62] and then updated in RFC2581[69]. The goal of adding congestion control mechanism is to prevent congestion collapse by finding a suitable transmission rate for each connection. For this purpose, an additional window limit called congestion window (cwnd) was introduced which varies based on the network condition. The effective limit on outstanding data, called "send window" (swnd), is set as the minimum value of the "receiver window" (rwnd) and cwnd. "Slow Start" and "Congestion

Avoidance" are two subsystems of congestion control mechanism that dynamically prevent congestion collapse [62].

Different extensions of TCP have dissimilar policies in dealing with packet losses. Tahoe detects packet loss by timeout and it takes as a sign of congestion. Therefore, Tahoe takes half of the current window as the new slow start threshold, set the congestion window to one and retransmit all unacknowledged packets. Tahoe increases the window additive by 1 while the window size is less than threshold and by 1/window thereafter.

The goal of NewReno-TCP approach is the ability to detect multiple packet losses. In the event of a packet timeout it only retransmitted the first unacknowledged packet, threshold will be reduced by half and the window will be set to half of the old window size plus three. NewReno remembers the highest packet number in the old window and when all the packets on the old window acknowledged by receiver, sets the congestion window threshold value and continues congestion avoidance like Tahoe.

TCP with 'Selective Acknowledgments' is an extension of TCP NewReno which is able to detect multiple lost packets and re-transmission of more than one lost packet per Round Trip Time (RTT). In SACK approach segments should be acknowledged selectively instead of cumulatively. Each acknowledged has a block which represents the segments are being acknowledged. Also TCP SACK only transmits the segments when number of outstanding packets in the path is less than congestion window size.

Similar to TCP, SCTP congestion control uses two mechanisms, slow-start and congestion-avoidance. At the slow-start mode, the congestion window is steadily increased and until it exceeds certain threshold it switches to congestion-avoidance mode. In slow-start, the congestion window is increased by a minimum of one MTU per received SACK chunk, and in congestion-avoidance phase, it is only increased by one MTU per RTT. As in TCP, SCTP uses two mechanisms to detect loss: "Fast Retransmit" and "Retransmission Timeout". SCTP's Fast Retransmit algorithm is slightly different from TCP's. SCTP's fast retransmit is triggered by four SACK reports instead of three duplicate ACKs in

the case of TCP. The outcome of retransmission is the reduction of the threshold to the size of congestion window and reset the congestion window to one MTU.

A wired-cum-wireless topology is used to study the performance of SCTP along with other extension of TCP including Tahoe, NewReno and SACK. The aim of this phase of simulation is performance comparison for all these transport layer protocols at the presence of mobility and packet loss. In the simulations, the congestion window, the throughput (defined as number of total bits transferred per time unit) and the goodput (defined as number of actual useful data transferred after removing headers and retransmissions) in different handover scenarios are simulated.

The second set of simulation is allocated to consider the benefit of the multi-homing feature of SCTP in different handover scenarios. In a handover based on multi-homed feature of SCTP the connection to new coverage area will be set up before the current communication is disconnected within the overlap area of adjacent cells.

And finally in the last set of simulation, nSCTP, the new proposed protocol, is implemented and the performance of this protocol is compared with the NEMO basic support protocol.

6.1. Network Simulator 2

The chosen discrete-event simulator is the Network Simulator (NS-2) [70]. NS-2 is an open-source simulator widely used in the academic community. Therefore, many people are working on this project and there is a wide variety of add-ons. NS-2 is implemented in two parts: a TCL interpreter to make the simulation scripting easier and a C++ implementation to have faster simulations. Figure 6-1 shows a simplified user's view of NS.

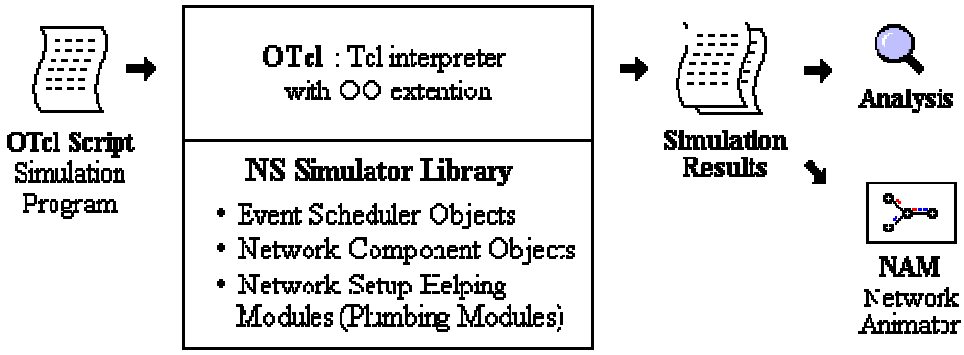

Figure 6-1: Simplified User's view of NS, taken from[71]

TCP is widely used in reliable communication over private and public networks. A partially implemented version of TCP agent is available in NS-2. Different types of TCP such as Reno, Vegas and SACK in NS-2 is supported only in one-way communication. A synchronization packet developed in NS-2 is only one way, sent from client and acknowledged by the server, and there is no synchronization packet sent in the opposite direction. Terminating the connection which is part of the standard TCP is not available in NS-2. Advertised window (AWND) mechanism is not part of the current version of NS-2 and it is supposed to be fixed, equal to twenty packets by default.

SCTP module is an agent developed for NS by the Protocol Engineering Lab [72] at the University of Delaware. The SCTP module has been added as part of the recent version of NS-2 (versions ns-2.29 and thereafter). SCTP module for NS-2, released with NS-2.29, supports limited multi-homing based on wired topology and end-to-end reliable transmissions. Some parts of SCTP like ADDIP and partial reliable transmission and full multi-homing scenario are currently not supported by this module.

NS-2 uses two type of addressing: flat and hierarchical addressing. Both addressing methods have been used in this chapter simulation. Flat addressing is mainly used for wired scenario. It consists of only one level of addressing. Hierarchical addressing scenario consists of 3 levels of addressing including domain address, cluster address and finally Node-ID which is similar to classified IP addressing using in the real network applications. In this simulation wireless scenarios used the hierarchical addressing method. In application layer,

File Transfer Protocol (FTP) is chosen for this simulation that needs TCP or SCTP in order to provide reliability.

To analyse the result of the simulation two method of visualisation have been used. In the first method, summarising and extracting the useful information from the standard trace file generated by NS-2, using AWK [73] programming language which is designed for processing text-based data either in files or data streams. And the second method is using network animator (NAM) tool part of NS-2 package for viewing network simulation traces and real world packet trace data.

6.2. Vertical Handover with the Basic SCTP

In this section, different transport-layer protocols are used in the vertical handover scenarios. In this simulation, Random WayPoint (RWP) similar to many previous studies [74],[75] has used as mobility model. Random waypoint is a simple model that is easy to implement and analyse. In the RWP model, the nodes or mobile users, move along a zigzag path consisting of straight legs from one waypoint to the next [74]. Based on this mobility model, the goodput is measured for different transport-layer protocol and results are compared. SCTP is simulated without enabling the multi-homing feature. The objective of this simulation is to analyse the potential benefit of using SCTP in a combined wired and wireless scenario at the presence of mobility and error on the communication links.

6.2.1. Simulation Scenario

The scenario consisted of:

- A single mobile node placed in a 670m by 670m rectangle, using the Random Waypoint mobility model and working as a sink client to collect FTP traffic from the corresponding node (see Figure 6-2)
- Four base stations two of them belong to HA domain and the other two of them belong to FA domain in order to provide both inter-domain and intra-domain handovers. They are distributed as shown in Figure 6-3

and each base station is able to handle a transmission range of up to 250m (see Figure 6-3)

- Four routers, with following functionalities: (See Figure 6-2)
  - Internet Service Provider (ISP) router is an access router that connects the corresponding node to the public network.
  - Gateway router is a backbone router that connects the mobile network to the public network or the Internet.
  - Home Agent (HA) is part of the mobile network components which provides the facility to allocate an address to the MN and tunnels the packets towards the current position of the MN.
  - Foreign Agent (FA) is part of the mobile network components which belongs to a different domain of the HA. Its function is to provide a CoA for the MN, informs the allocated CoA to the HA and the CN and finally handle the traffic to/from the MN when the MN is located inside the coverage area of the FA.
- Correspondent Node, works as a server to generate FTP traffic. In the simulation, different transport agents provide a reliable connection from this node to the MN.
- All wired links have a bandwidth of 5 Mbps. A TCP connection (or an SCTP association) is used to transport the data generated by the FTP.

The total simulation time is 200 seconds. Tahoe, New Reno and SACK enabled versions of TCP were used for the simulations. The MTU for each link was kept at 1500 bytes. The TCP segment size and SCTP data chunk were kept at 1000 bytes. The initial congestion window size for both TCP and SCTP were kept both equal to 2*MTU. The speed of the MN was a random value between 0 and 30m/s using a random waypoint mobility model. The base stations were distributed in a 670m square as shown in Figure 6-3 to have the maximum coverage in the region.

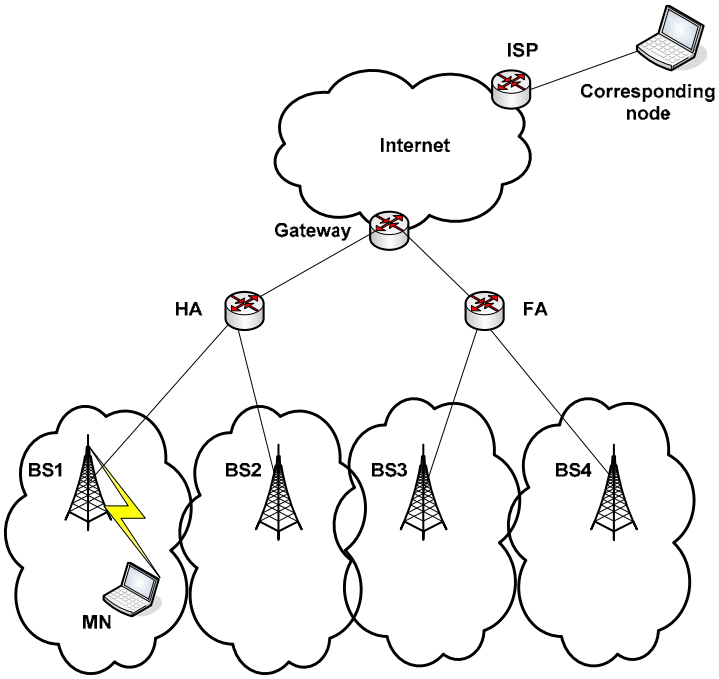

Figure 6-2: Simulation Topology in a wired-cum-wireless scenario

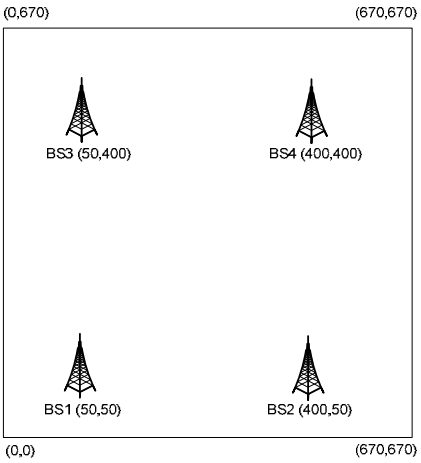

Figure 6-3: Distribution of BSs in a 670m*670m area

6.2.2. Packet arrivals Comparison

In order to analyse the connection robustness, a number of experiments have been done to compare the received data for different versions of TCP and SCTP when the MN has a RWP mobility model. Figure 6-4 shows the aggregation of the received data during the simulation time in two different scenarios. In the error-free environment all the TCP extensions delivered almost similar amount of data. TCP-Tahoe, TCP-NewReno and TCP-SACK have similar mechanisms for preventing congestion collapse and finding an appropriate rate of transmission for each connection dynamically. SCTP shows slightly better data delivery rate

compared to various versions of TCP in the simulation as congestion control algorithms for both TCP and SCTP are similar. The difference in data rate between SCTP and TCP is due to the NS-2 implementation of TCP and SCTP.

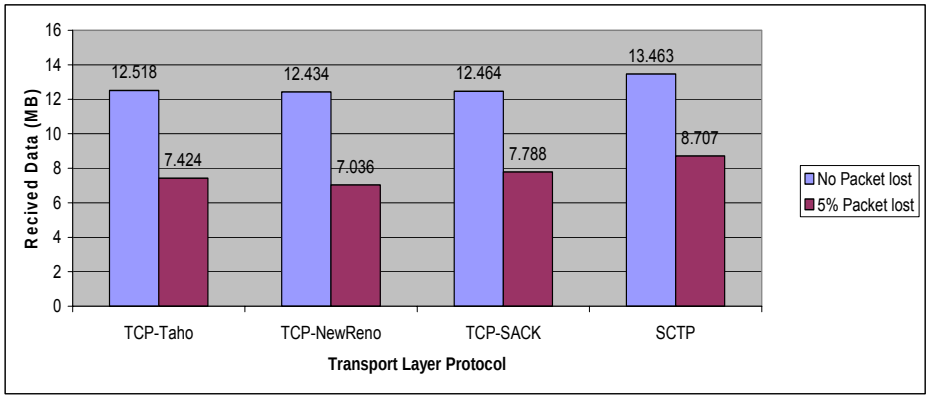

Figure 6-4: Comparison of aggregation received data in zero drop and 5% loss rate scenarios

The main differences between these protocols are in congested and high error-rate scenarios that the packets are subjected to drop or loss. The results show TCP-SACK has better performance when a high error-rate was applied in the wireless path. The SACK-enabled segments provide the TCP sender with some extra information of the status of the destination's receiving buffer. In SACK for every received packet, the receiver produces a reply which contains further information in the header of the segment in the form of an option. Hence, in the event of packet loss the sender can resend only the exact packets that have been lost in transit and avoid producing unnecessary retransmission. TCP-NewReno produces least performance as it primarily optimised to work with the burst error scenarios. SCTP shows better performance compare to TCP-SACK in the same situation. Original SCTP does not include a Fast Recovery mechanism, as found in NewReno-TCP and SACK-TCP and later TCP variants. As specified in RFC2960 [3], "because cwnd in SCTP indirectly bounds the number of outstanding TSN's, the effect of TCP Fast Recovery is achieved automatically with no adjustment to the congestion control window size". This built-in fast recovery system along with the benefit of SACK algorithm implemented in SCTP makes this protocol robust in high error-rate scenarios.

Figure 6-5 and Figure 6-6 show the aggregation of packet arrivals at the MN. The stationary parts on the curves indicate disconnectivity at that point, which are the impact of handovers at specific times.

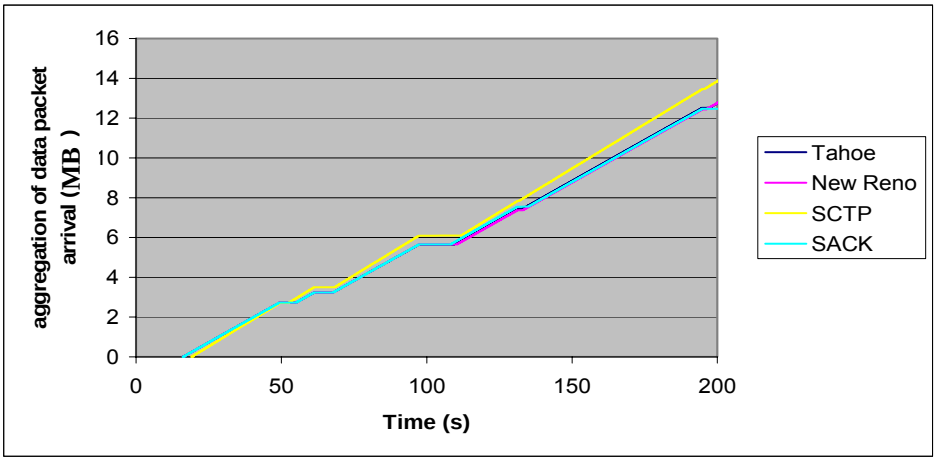

Figure 6-5: Comparison of aggregation data-packet arrival in different transport layer protocol with handovers based on MIP in an error-free environment

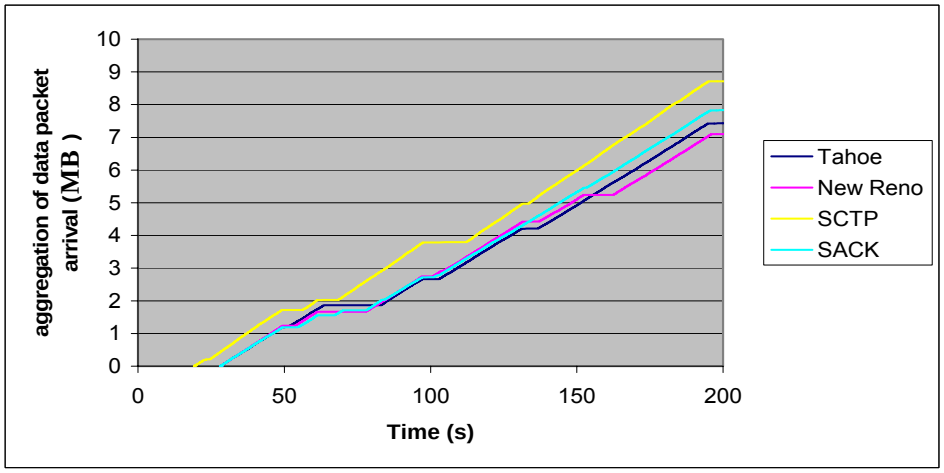

Figure 6-6: Comparison of aggregation data-packet arrival in different transport layer protocol with handovers based on MIP and 5% uniform packet losses

The results presented in Figure 6-5 and Figure 6-6 show that the current SCTP implementation performs almost as well as TCP when there are no losses. However, SCTP seems to perform better in the presence of losses, as it benefits form built-in fast recovery system and does not enforce strictly ordered delivery. TCP guarantees in-order delivery of data to the application layer within a single

TCP session. Therefore, TCP detects a gap in the received sequence number and has to wait to fill this gap. While, SCTP can deliver data to its upper layer protocol even if there is a gap in TSN if the Stream Sequence Numbers are in sequence for a particular stream. This event does not affect cwnd and only affect rwnd calculation.

6.3. Vertical Handover with Multi-homing Feature of SCTP

The main difference between SCTP and TCP is multi-homing. Multi-homing enables SCTP to establish robust communication associations between two endpoints and each of them could be accessible by more than one transport address. In a multi-homed SCTP, the sender usually uses the same destination address. The destination address could be changed either by instruction from the upper layers or the address becomes unreachable. Also, SCTP may retransmit to a different transport address than the original transmission. In a multi-homed scenario the sender keeps the congestion control parameter set for each destination addresses separately and in the case that the address is not used for a long time period the parameters will be deleted. Also, for each of the destination addresses, an endpoint does slow-start upon the first transmission to that address.

In this phase of the simulation, multi-homing feature of SCTP is investigated. In this simulation, traffic was sent between two nodes connected by two parallel links. Choosing different links' parameters enable us to observe how the multi-homing feature of SCTP deals with out-of-order segments and in addition monitor the progress of congestion window on each link separately. The main objective of this simulation is to understand the detailed operation of the multi-homing feature of SCTP and validate the behaviour of this protocol. Standard SCTP defines a HEARTBEAT signal that checks the availability of a channel in regular time intervals. The HEARTBEAT is sent when there is no knowledge of the link condition. At the start time of the transmission the association between SCTP sender and receiver, marked one of the available links as "primary link" that handles the actual data transmission between two ends. The other link(s) are used as alternative link(s) to the primary. These alternative links need to be

checked frequently using HEARTBEAT signals. When a packet loss is detected on the primary link, that packet will be retransmitted through the alternative link. Increasing the number of consecutive packet losses in the primary link will result in swapping the primary link with one of the alternative links.

6.3.1. Simulation Scenario

In this simulation only two paths are available between the sender and the receiver. These paths are defined as primary and secondary paths and at some specific time during the simulation changeover occurs. These two links were used to simulate handover scenarios between a high-bandwidth link (e.g. WLAN) and a low-bandwidth link (e.g. UMTS) in all possible combinations.

Similarly to the previous scenarios, an error-free environment and an environment with 5% random uniform packet loss have been used in the simulation. The simulation topology is shown in Figure 6-7. Two BSs are connected to different wireless access networks. The coverage areas of BSs have been set in which an overlap region is formed between adjacent cells in order to allow the handover procedures to be completed, as explained in section 2.5.2.

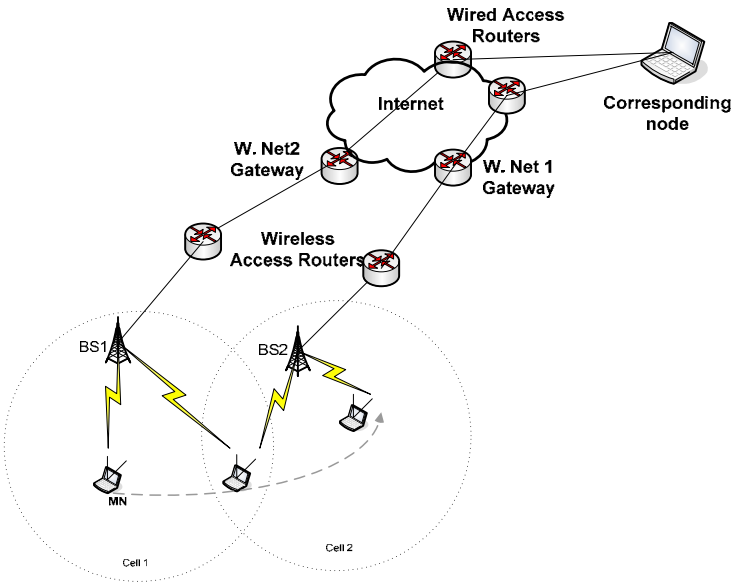

Figure 6-7: End-to-end multi-homed simulation topology

In this simulation, each end user has two interfaces and forming 4 set of SCTP associations. For simplification only two associations formed by (Core0-Inf0 ,

Core1-inf0) and (Core0-Infl , Core1-infl) have been addressed as shown in Figure 6-8 and the other two associations (Core0-Inf0 , Core1-infl) and (Core0-Infl , Core1-inf0) were not considered. The corresponding node is attached to Core0, and the mobile user is attached to Core1. The FTP traffic generator is attached to Core0 and the traffic is sunk at Core1. FTP starts at 500ms and the primary destination is set on "Link1" in Figure 6-8 at the beginning of simulation. All the important parameters for this simulation are summarised in Table 6-1.

Simulation Parameters	
Parameter	Value
Number of users	2
Simulation length	12s
Traffic	FTP
UMTS Bandwidth	0.5 Mbps
UMTS link Delay	200ms
WLAN Bandwidth	11 Mbps
WLAN link Delay	20 ms
Low error-rate	Uniform 1%
High error-rate	Uniform 5%
Links queue mode	Drop Tail

Table 6-1: Summary of simulation parameters

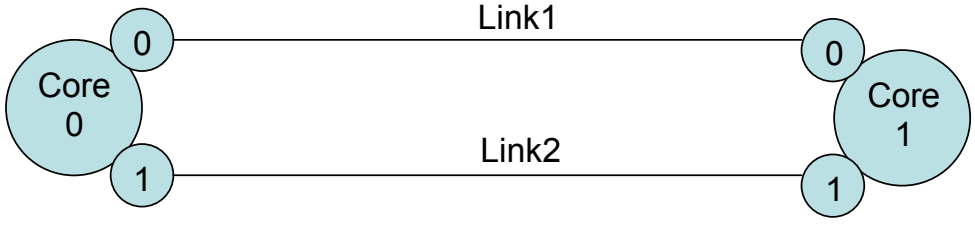

Figure 6-8: Structure of a multi-homed scenario implemented in NS-2

6.3.2. Error-Free Environment Scenario

In this set of the simulations a single handover in different link's condition while there is no error on the system have been simulated. A bulk FTP connection uses as application protocol on a multi-homed reliable SCTP and during the

transmission, the communication migrates from one link to the other. The timing parameters are summarised in Table 6-2.

Timing Parameters	
Time (s)	Action
0	Simulation Start
0	Set primary address on Link 1
0.5	FTP start
5.5	Primary address changes to Link2
10.5	FTP Stop
12	Simulation Stop

Table 6-2: Summary of timing parameters

Based on the type of wireless connections the following scenarios could be applied:

6.3.2.1. WLAN-WLAN Handover

When both links in Figure 6-8 have the WLAN link specifications, the aggregation of received data shown in Figure 6-9. This result shows the seamless handover between the two links as both links follow each other without any interruption in data transmission. As both links are defined as the same technology the progress of aggregation data over the simulation time is almost in the same gradient except at time of handover which service reduction can be observed. This reduction is due to slow-start mechanism, which is part of the congestion control strategy used by SCTP in order to avoid sending more data than the network is capable of transmitting.

SCTP congestion control has been derived from TCP, with an additional multi-homing feature. In a multi-homed SCTP, for each destination address a separate set of congestion control parameters is maintained, so from the network point of view, an SCTP association with N paths behaves similarly to N TCP connections. This also means SCTP congestion control can fairly share bandwidth with TCP on the same network.

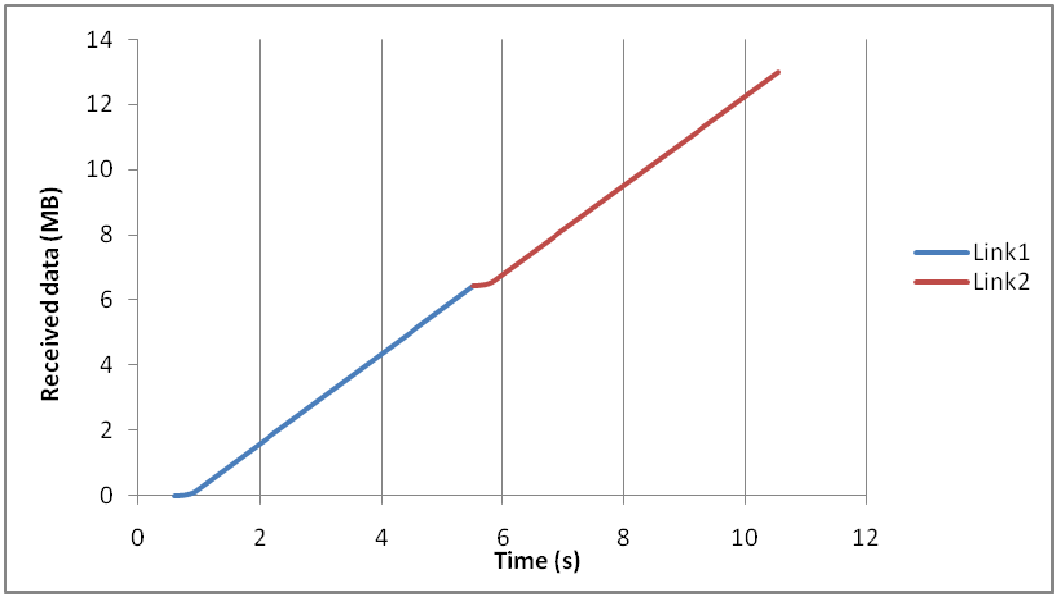

Figure 6-9: Aggregation of received data

The result on Figure 6-10 is more revealing, showing that the congestion window in the primary link remains substantially large even after the alternative link takes over. SCTP defines two different congestion windows for the two links and they are working independently. The graph also shows, after transmission starts on the new link (Link2) all the packet were waiting on the sender queue are still sending out.

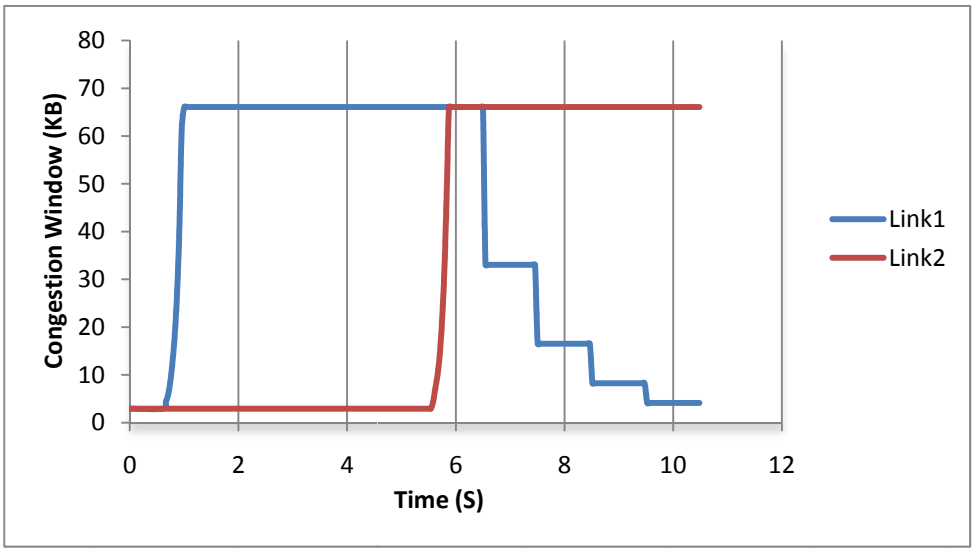

Figure 6-10: Effect of congestion window in multi-homed situation

6.3.2.2. UMTS-UMTS Handover

A similar result with the previous scenario is expected for the condition that both links are set on UMTS link parameters. As transmission delay in UMTS links is higher than WLAN links, at the handover time some of the packet from the new link (Link2) will arrive before the queued packets on the old links, as shown in Figure 6-11. The impact of handover on the congestion windows for Links 1 and 2 are depicted in Figure 6-12. This result confirms that the new link goes through the slow-start procedure of SCTP before the old link shuts down completely.

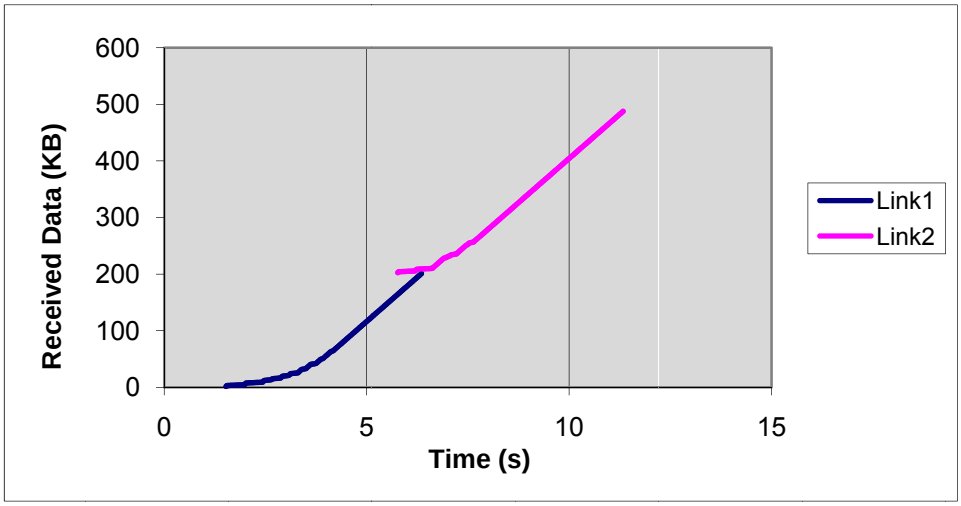

Figure 6-11: aggregation of received data

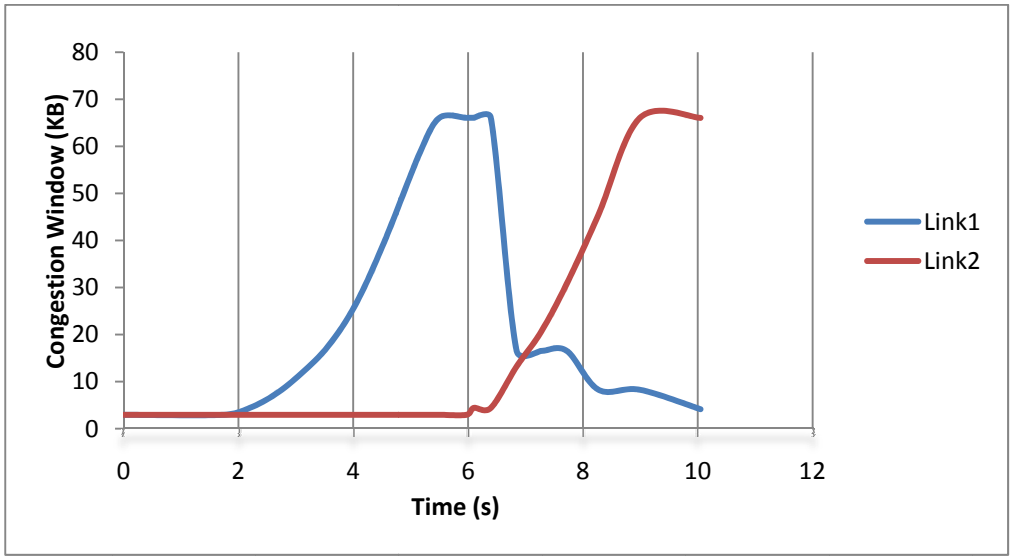

Figure 6-12: Effect of congestion window in multi-homed situation

6.3.2.3.WLAN-UMTS and UMTS–WLAN Handovers

In some of the cases handover is from a high bit-rate link (e.g. WLAN) to a low bit-rate link (e.g. UMTS) or vice versa. An example of this scenario is when a MN which is already connected to a UMTS mobile access technology, enters into the area with WLAN-AP coverage and to use the benefit of high bit-rate transmission compared to UMTS, it switches to the WLAN access technology. Also, as the MN leaves the WLAN coverage area in order to keep the connectivity it needs to switch back to the UMTS. A similar configuration as presented in section 6.3.1 is used and the links are connected through the WLAN and UMTS wireless access technologies. Figure 6-13 shows the behaviour of bulk data transmission when the primary link is WLAN and secondary link is UMTS. In this situation a heavy reduction of service can be observed. A heavy reduction of data rate as well as higher transmission delay for UMTS caused a gap or disconnectivity in transmission. While, as it is shown in congestion windows for both links (see Figure 6-14) the transmission will not be terminated before link2 starts data delivery.

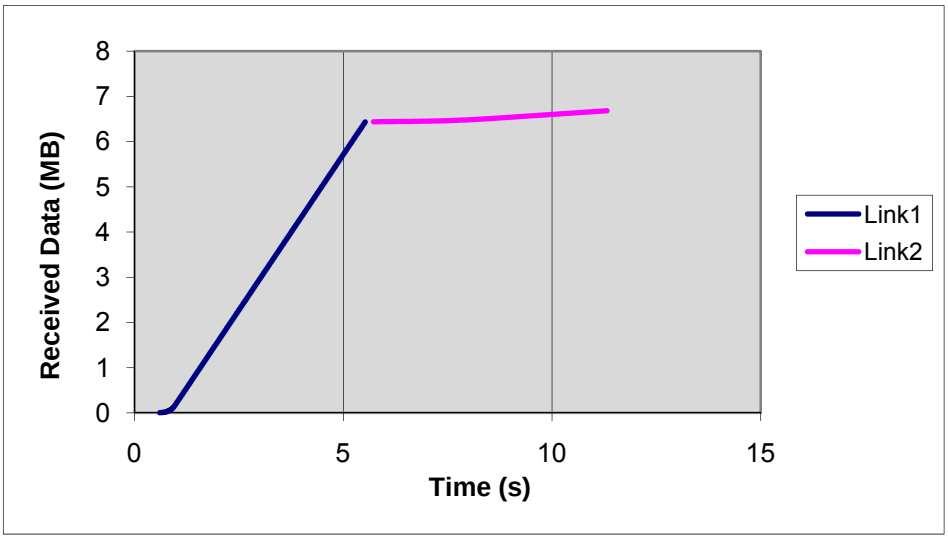

Figure 6-13: aggregation of received data

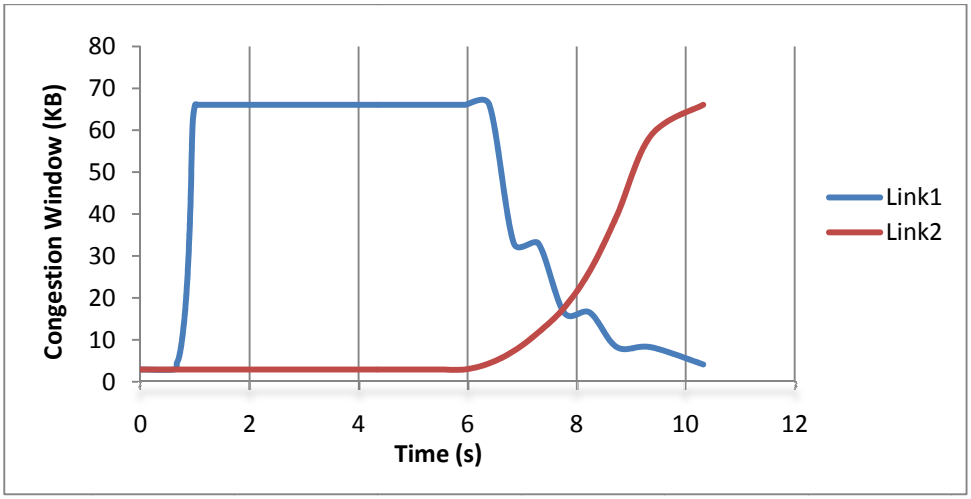

Figure 6-14: Effect of congestion window in multi-homed situation

Migration from a low bit-rate link to a high bit-rate link is shown in Figure 6-15 and Figure 6-16. As observed, packets through link2 will arrive to the destination before the packets queued on transmission buffer of link1. As a result the out-of-order delivery at the receiver must be addressed that could be easily compensated by retransmitting via link2 that benefits from a lower latency and higher bit-rate.

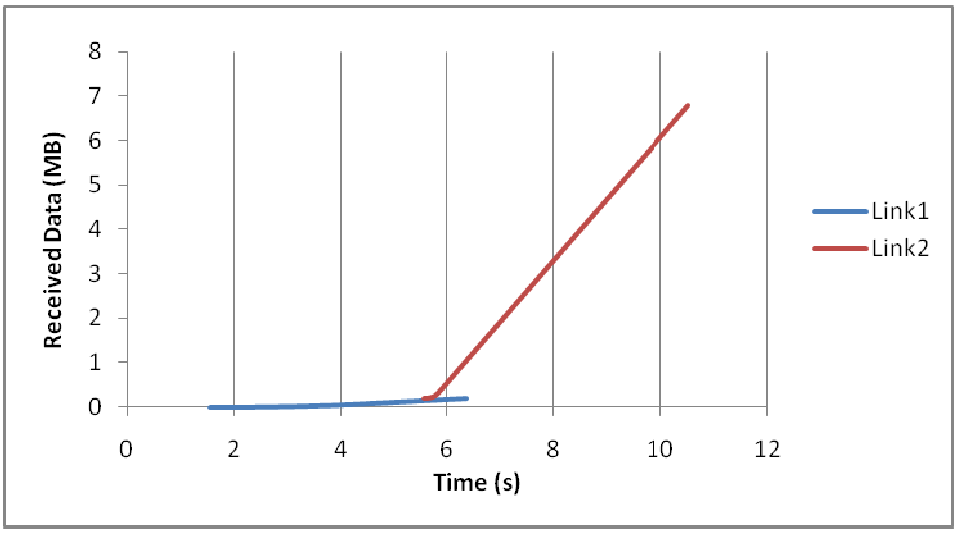

Figure 6-15: Aggregation of received data

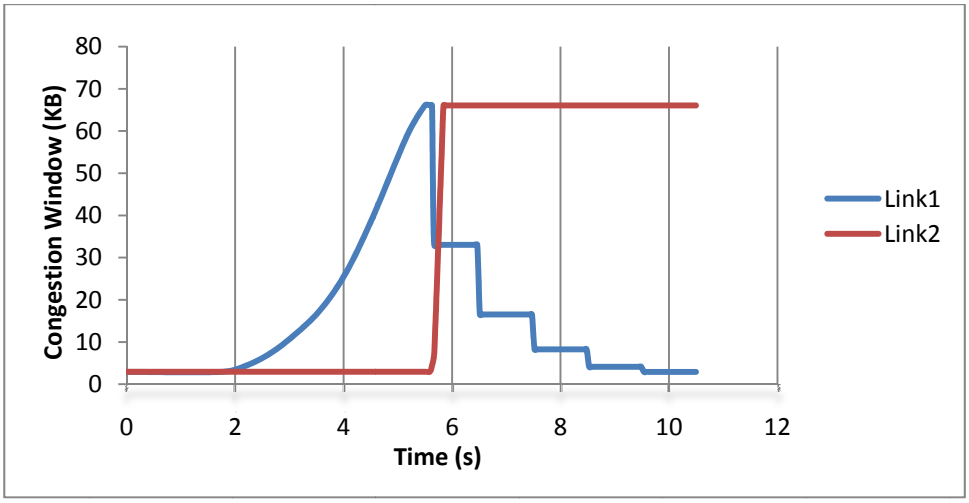

Figure 6-16: Effect of congestion window in multi-homed situation

6.3.3. Scenarios with Random Errors

In this part of the simulation, links with uniform error model are considered. In realistic situations, the bit errors on wireless links depend on the interference from other wireless devices, the distance from the sender, the natural and artificial obstruction, shadowing and many other features of the radio medium. For simplicity, we model the instability on channels with a uniform error model available in NS-2. This error model uses a uniform distribution with a specific error-rate (1 to 5 percent in this simulation) randomly drops packets sent on the link. However a uniform error model does not reflect the reality of a wireless channel well, as some errors are bursty for wireless channels but the aim of this example is to show the behaviour of multi-homed SCTP in a high error-rate environment. The length of simulation is 30 seconds and one handover is experienced and set to occur almost in the middle of the simulation time. Table 6-3 shows the simulation parameters.

Timing parameters	
Time (s)	Action
0	Simulation Start
0	Set primary address on Link1
0.5	FTP start
17.5	Primary address changes to Link2
29.5	FTP Stop
30	Simulation Stop

Table 6-3: Summary of timing parameters

In a multi-homed SCTP if a packet loss occurs, the alternative link will retransmit the lost packet. Similar configuration as presented in Figure 6-8 is used to study the behaviour of multi-homed SCTP at the presence of handover while different error-rates are applied on the communication links.

Throughout the simulation the following handover scenarios were monitored: WLAN-WLAN handover response is shown in Figure 6-17 that the new link has less error-rate compared to the old one therefore, as it observes the gradient of the lines on the "New WLAN" is more than "Old WLAN" and consequently a higher transmission rate is expected on the "New WLAN". Aggregation of received data in the case of UMTS-UMTS handover scenario is shown in Figure 6-18 where both links experience a 5% error-rate. And finally WLAN-UMTS that represents migration from a high bit-rate WLAN link to a low bit-rate connection is shown in Figure 6-19 and as it is expected transmission rate on old link is much grater than the new link.

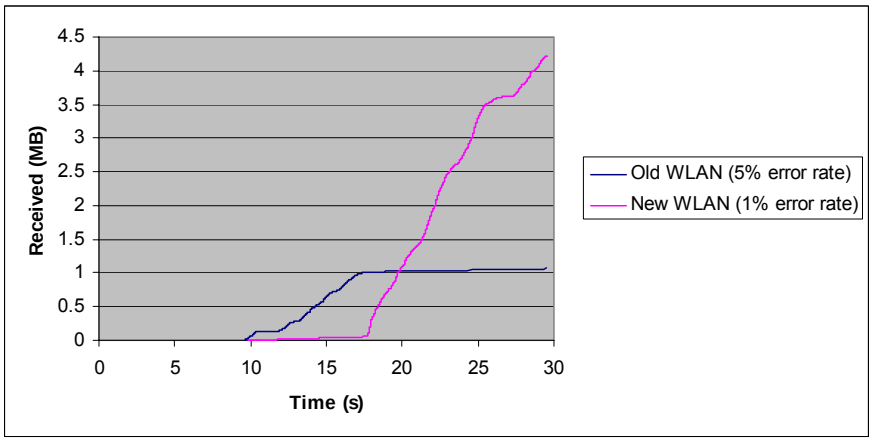

Figure 6-17: Aggregation of received data in a WLAN-WLAN Handover with different error-rate on the links

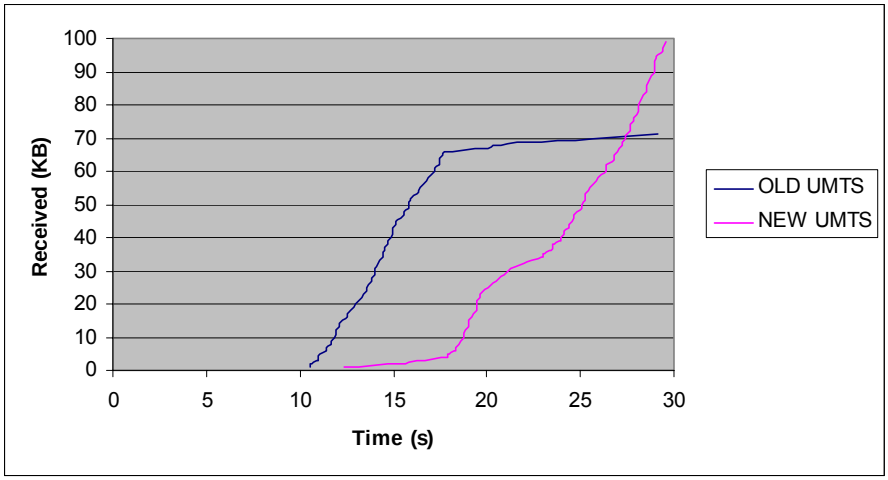

Figure 6-18: Aggregation of received data in a UMTS-UMTS handover with 5% error-rate on both links

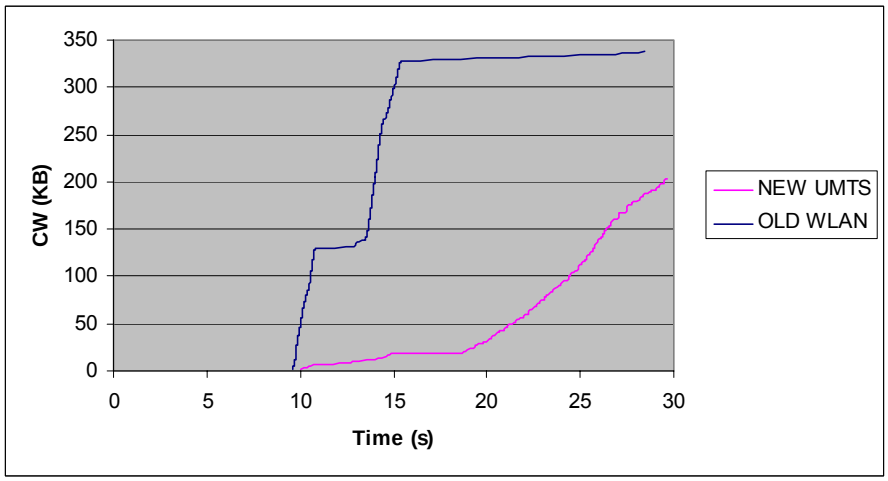

Figure 6-19: Aggregation of received data in a WLAN-UMTS Handover with 5% error-rate on both links

In all three experiments the transmission starting with delays at the beginning and that is due to errors occurring, is unlikely at the association and handshaking phase of transmission. Also both links are involved in communications through the entire time of the simulation, which is the result of SCTP reaction to the lost packet which is retransmitted through the alternative link.

6.4. Links with sudden breakage

In the previous sections the conditions with handover decision were considered. It was mentioned that at the specific time in the middle of the overlap area of both links, the SCTP association negotiates the handover time. Those scenarios are the normal movement condition that most of the time are the case for any mobile devices involved in the communication. In this simulation a sudden link breakage will be considered and the way that multi-homed SCTP deals with these circumstances will be studied. A real world example for this scenario is the condition that multi-interface MN is placed in an office within WLAN and UMTS coverage (see Figure 6-20). With the assumption that default connection is the WLAN and the UMTS is used for backup or alternative link, this MN communicates with a corresponding node. The SCTP association contains both interfaces at each end.

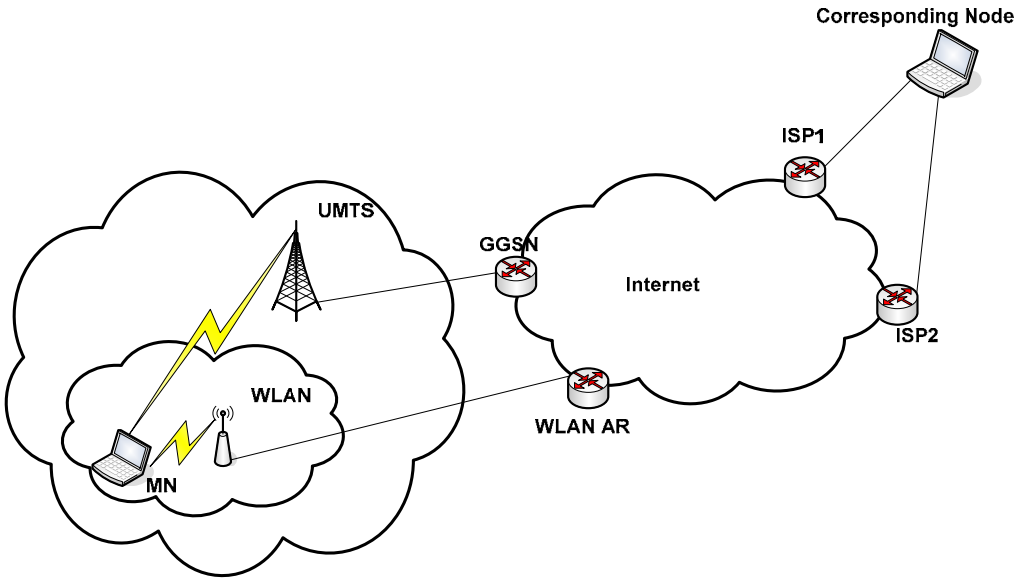

Figure 6-20: Network Topology

During the file transmission, a link failure occurs in the WLAN connection. In this situation, there is no previous negotiation in the SCTP association between the MN and the corresponding node to change the primary link. The consequence of this breakage will be interruption in data transmission and all the packets and acknowledgements in transit are subject to loss. The aim of this simulation is study on recovery time to establish the connection with the other available link and the variations of congestion windows in both links.

In this scenario, the MN is assumed to be stationary and while a bulk transmission using multi-homed SCTP agent are operating on the WLAN interface, the connection breaks and again after a period of time the WLAN link will be resumed. Therefore, smooth handover on the recovery from WLAN to UMTS is expected.

For implementation, the multi-homed topology described in section 6.3.1 was employed. Method “down” inside “rtModel” class of NS-2 is used to simulate the link breakage at specific time. The timing and specification of this topology and scenario are shown in Table 6-4.

Simulation Parameters	
Time 0	Simulation Start
Time 0	Set primary address on Link1
Time 0.5s	FTP start
Time 3.0s	Link1 breaks
Time 6.0s	Link1 resumes
Time 8.5s	FTP stop
Time 9.0s	Simulation Stop
Link 1	Wireless Link
Link 2	UMTS link
WLAN Bandwidth	2Mbps
WLAN Propagation delay	20ms
UMTS Bandwidth	0.4Mbps
UMTS propagation delay	100ms

Table 6-4: Simulation Parameters

Simulation results are shown in Figure 6-21 and Figure 6-22 that represent the aggregation of received data during the simulation time and the progress of congestion windows for both links respectively. At the time 3 seconds the WLAN link breaks and transmission will be stopped and congestion window dropped to Zero. As specified in RFC2960 [3] when its peer endpoint is multi-homed, an endpoint should keep an error counter for each destination. Each time the packet loss on any address, or when a HEARTBEAT sent to an idle address is not acknowledged within a retransmission time out, the error counter of that destination address will be incremented. When the value in the error counter exceeds the protocol parameter 'Path.Max.Retrans' (three for this simulation) of

that destination address, the endpoint should mark the destination transport address as inactive. Therefore, the transmission will be moved on the UMTS link. Transmission will be carried on through UMTS link where the lost segments and the segments belonging to the lost acknowledgments must be retransmitted. And finally when the WLAN connection resumes at 6 seconds a seamless handover to WLAN is observed.

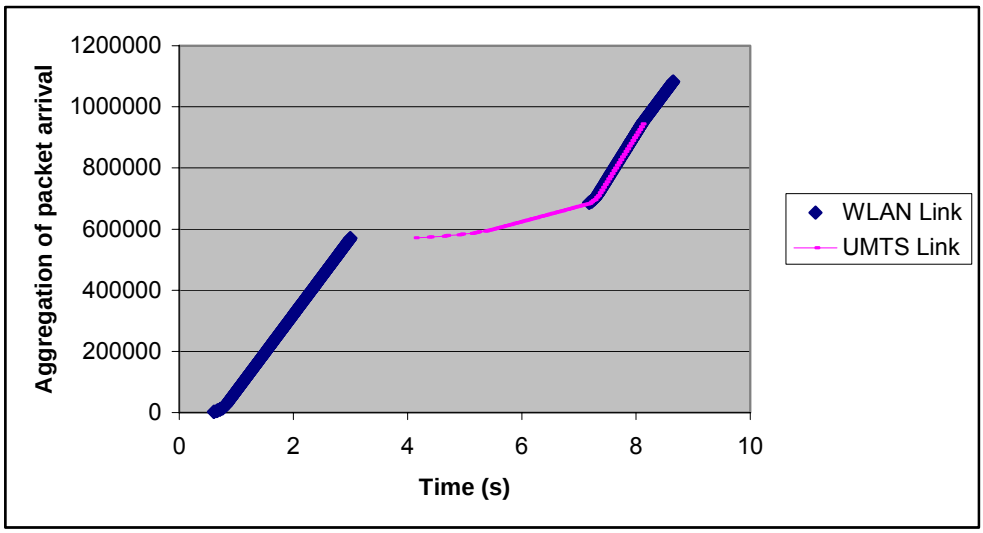

Figure 6-21: Packet-arrival rate in the sudden link-breakage scenario

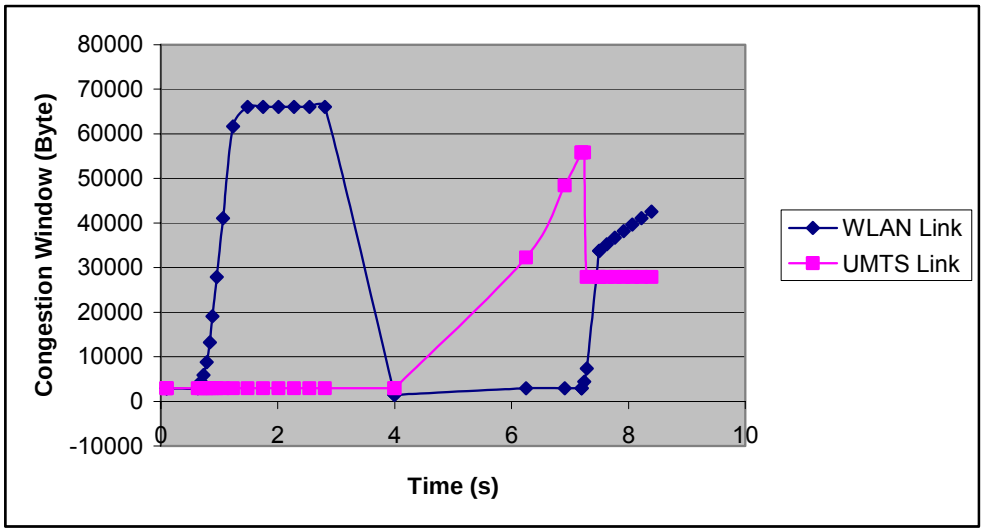

Figure 6-22: Congestion window size in the sudden link-breakage scenario

6.5. nSCTP Simulation

In this section the performance of our proposed protocol, nSCTP, will be investigated through a simulation study with NS-2. Figure 6-23 depicts the implemented topology in the simulation platform. The communication between the CN and the MN passing through a transport layer SCTP tunnel that should be setup between the MR-HA and the MR. For simplification an end-to-end SCTP connection with multi-homing feature runs on both ends. The same topology has been used to evaluate the performance of NEMO that uses MIP to handle the handover. The mobile router has two interfaces with multi-homed SCTP that will be used to perform handover however, just one interface is used in the NEMO architecture.

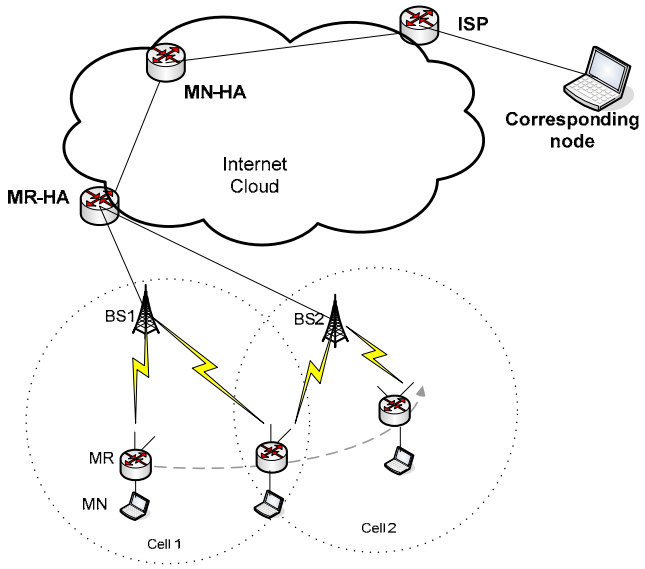

Figure 6-23: Simulation Topology

In the simulation, we aim to compare the throughput and goodput of nSCTP and NEMO. The throughput is defined as the number of successful bits transferred between the CN and the MN. Consequently, the goodput is the number of useful data bit transferred regardless of packet header and signalling control. The IP header sizes in all experiments are based on IPv6. Header for SCTP segments that should contain at least one chunk has been set to 16 bytes.

Figure 6-24 shows the simulation result for the explained topology in Figure 6-23 when the handover is between two WLAN cells with the data rate of 11Mbps that are shared with both control and data packets.

Movement scenario, which is applied to mobile router, follows a ping-pong mobility model between cell one and two. The number of handovers shown in the x-axes and the average data rate are placed in the y-axes.

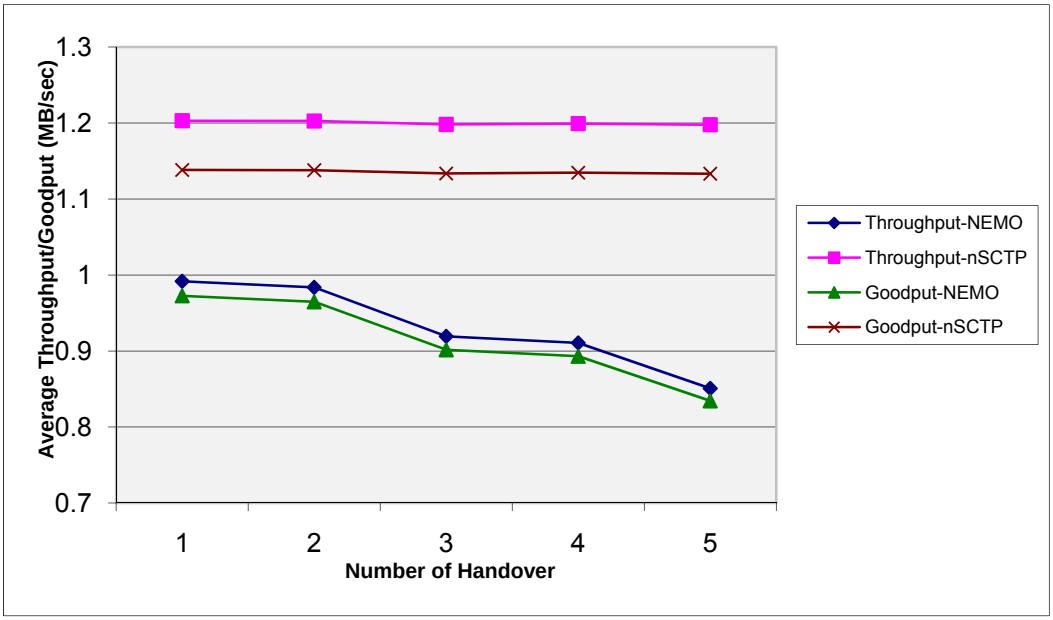

Figure 6-24: Comparison the results of the nSCTP and NEMO handover

From the simulation results presented in Figure 6-24 the overall throughput and goodput in nSCTP is larger than in NEMO. The difference between throughput and goodput in nSCTP is almost three times more than that of NEMO. That is due to an additional transport layer tunnelling on the new proposed protocol compared with NEMO. By increasing the number of handovers the level of bit transferred will be reduced in both nSCTP and NEMO, but the amount of this reduction for nSCTP is much smaller than NEMO. Therefore, increasing the number of handovers has a minor impact on the performance of nSCTP. NEMO, regardless of having smaller amount of packet overhead in transmission, is not able to cope with handover in a smooth manner and increasing the number of handovers significantly reduced the performance of this protocol.

6.6. Chapter Summary

The proposed multihoming mobility management for moving networks, nSCTP, was simulated in this chapter. For that purpose, three sets of simulations were studied within the NS-2. Firstly, we showed that in the non-multi-homed support situation (e.g. single interface MN), SCTP can work at least with the similar performance of other reliable transport layer protocols including Tahoe-TCP, NewReno-TCP and SACK-TCP. In the simulations, a combined wired-wireless topologies were implemented and the performance of SCTP and the above TCP extensions with a bulk FTP transmission and their congestion windows behaviour were studied. Different scenarios consisting of vertical handovers and uniform error-rate were taken to experiment. The simulation results show that there is no major improvement introduced by using SCTP in these circumstances. This is not an unexpected result, as SCTP follows an almost similar congestion control mechanism and fast recovery as TCP does and the main innovation of SCTP is where new features such as multi-homing and multi-streaming, are being used. However, SCTP seems to perform better in the presence of losses, as it benefits from a built-in fast recovery system and does not enforce strictly ordered delivery.

In the second set of the simulation the multihoming feature of SCTP which has been used to smooth the handover management was simulated. A variety of handover scenarios have been done to show this scheme can deal properly in different circumstances. The results were more promising as they clearly show significant improvement could be achieved in handover latency. That is the main contribution of transferring more data during the simulation time.

Finally, nSCTP and NEMO were implemented and they have been tested in a ping-pong scenario and the throughput and the goodput were studied. The result shows however nSCTP apply more overhead on the system but the number of bit transferred in nSCTP is higher than NEMO. This difference will be dramatically increased as the handover-rate increases in the network.

In the previous sections of this chapter SCTP protocol as reliable transport protocol in a combined wire and wireless network environment was studied. The multi-homing features of SCTP which can be used to smooth the handover

management were described in section 6.3 and followed with the analysis of the effect of this mobility management protocol on sudden link breakages in section 6.4. The primary results from these sections were shown the performance of multi-homed SCTP on different scenarios.

Chapter 7. QoS Provisioning in SCTP

In the previous chapters the importance of involving a new transport layer protocol called SCTP in mobile communications has been considered. SCTP's Multi-homing feature addresses the problem of link failures by allowing a transport layer session to bind multiple IP addresses at each end point of communication. This feature provides both endpoints with multiple communication paths, and thus gives them the ability to failover (switch) to an alternate path when a link failure occurs. The simultaneous connectivity can be achieved in a heterogeneous environment by using multiple ISPs or multiple access technologies, such as cellular networks (e.g. GPRS, UMTS) and wireless LANs and MANs (e.g. 802.11, WiMAX).

Based on above information and in the interest of adapting SCTP with networks in motion scenarios, nSCTP has been developed and its performance and efficiency were studied. However, If the mobile routers were allowed to switch between available technologies based on their mobility, for example to take advantage of a high-bandwidth and low-cost service available in a limited area (such as a WLAN hot spot), then perceived service quality would be further improved.

In spite of all benefits and advantages of SCTP and consequently nSCTP, the failover mechanism of these protocols does not adapt well to application requirements or network conditions. In other word an association will insist to stay with a current primary link until it is disconnected completely or a certain number of consecutive time-outs are experienced, however some better quality links through other wireless access technologies could be available.

In this chapter, the important parameters that could be involved in a policy based handover such as available bandwidth and number of packet loss were studied. The algorithms for reading these parameters on primary and alternative links are presented and based on obtained information different policies for handover were presented. To monitor the condition of alternative links on an SCTP association a

dual heartbeat technique is proposed. In this technique a pair of heartbeat signals back-to-back sends to the peer node through all available paths in an SCTP association to periodically check the availability of each path and also estimates the end-to-end delay and available bandwidth.

The signalling required to periodically obtain the necessary parameters on the paths, injects some new communications overhead as well. This resulted in unnecessary handover which will dramatically reduce the performance of our new proposed policy based handover scenario. The efficiency of this protocol has been tested by implementing a simulation model on the NS-2 platform. The result depicted that dynamic handover can significantly improve the efficiency of SCTP handover particularly in the area with different choice of wireless access points and mobility which can frequently affect the quality of received signals.

7.1. Bandwidth Estimation Techniques at Transport Layer

This section describes some of the existing bandwidth estimation techniques that calculate approximately the capacity and available bandwidth in an end-to-end connection which is running a reliable transport protocol like TCP or SCTP.

7.1.1. Single Packet Technique

In this technique bandwidth is estimated for an end-to-end connection based on measuring the capacity of each hop along a path by using the actuality that transferring a packet on slower links takes longer than faster links. This method firstly proposed by Bellovin [76] and improved in several ways such as [77] and [78].

This technique uses Time-To-Live (TTL) field of IP header to find an estimation of particular hop within a communication path. The value of TTL decrements by one when it passes through each router and when this value reaches zero a timeout error will be sent back to the router. In other words, the value of RTT for each router is calculated and the difference of two consequence routers gives the time that it takes for a packet to travel between these two nodes.

7.1.2. Packet Pair Technique

This technique is used to estimate the capacity of the bottleneck link of an end-to-end transmission path. In this method two packets of the same size send back-to-back. These packets experience some delay as they are passing through low capacity hops within the path which have consequence in creating a gap between the transmitted packet pair at the receiver. Calculating the time distance between these two packets will estimate the minimum available bandwidth in the path. Packet pair technique has proposed, used and improved in many ways since 1993 in some literature such as [15, 79, 80].

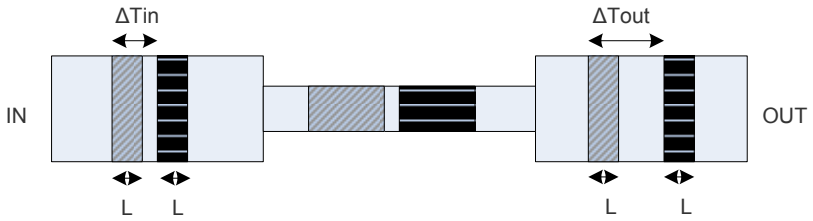

Figure 7-1: Packet pair operation

Figure 7-1 shows the operation of packet pair technique. Two packet of the same size are travelling from source to destination and through each hop they experience either equal or larger time difference. The outcome of $\Delta T_{out} = \Delta T_{in}$ shows that all hops provide sufficient bandwidth and there is not a hop causing bandwidth reduction on the path. Also, the result of $\Delta T_{out} > \Delta T_{in}$ is the consequence of existing at least a bottleneck hop within the communication path. As the path is forming by a series of hops in a communication system therefore the total link bandwidth will be set on the minimum bandwidth of each individual hops. Or,

$$BW_{Max} = Min(BW_1, BW_2, BW_3, BW_4, ...) \tag{7-1}$$

Therefore, the maximum data rate supported by the communication link or path is calculated by:

$$BW=L/\Delta T \tag{7-2}$$

Where BW is the bandwidth of the bottleneck hop or the maximum bandwidth that can be provided by the path, L is the length of the packets and time difference (ΔT) is:

$$\Delta T=\Delta T_{out} - \Delta T_{in} \quad (7\text{-}3)$$

7.2. Important Parameters on a Policy Based Handover

Traditional SCTP uses multi-homing as an alternative path to retransmit the unsuccessful delivered packets. Also, a certain number of consecutive packet losses will cause swapping of the primary paths to an alternative path. This feature along with ADD-IP extension of SCTP [7] formed some of the transport layer handover managements such as mSCTP [8] and nSCTP[9]. Traditional failover mechanism of SCTP however provides a soft and seamless handover but the number of packet losses during the handover is still high. In addition the availability of alternative paths in an SCTP association is periodically checked by sending the HEARTBEAT chunks on these paths, however this association is not aware of the paths' conditions.

Best path selection in a multihoming environment has been studied in several papers. Fracchia et al. [81] introduced a sender side transport layer protocol to estimate the available bandwidth that uses SCTP flexible path management features to change the active path. They used packet trains with different sizes to estimate the available bandwidth on each links which involves a huge number of signalling and overhead in the system. Also some issues such as time stamping and clock synchronization have not been addressed. In a different work [82] time intervals based bandwidth estimation technique is introduced which can particularly improve the TCP congestion control performance on a wireless link. In [83] QoS management at the transport layer for time sensitive application is proposed which is based on error recovery and dynamic playback management.

A policy based handover scheme could include one or all of the following QoS parameters:

- **Latency:** end-to-end delay is one of the main parameters for time sensitive applications. The response time for the real time applications

should be guaranteed so data is received at the destination within an appropriate time. Voice and video streaming are examples of these applications which usually use datagram transmission, which offers an unreliable service and many datagrams arrive out-of-order.

- **Bandwidth:** Bandwidth is a measurement of the running data from one computer to another. Bandwidth is directly proportional to the amount of data transmitted or received per time unit. The amount of bandwidth is important especially for a bulk data transmission and for this group of applications opposite to time dependent applications, the reliability and in-order data delivery are key factors.
- **Jitter:** defined as delay variation or how much the end-to-end network latency varies from time to time due to effects such as network queuing and link failures, which will cause the alternative routes to be used.
- **Loss ratio:** defined as the ratio of packet loss to the successfully delivered packet from source to destination.
- **Error-rate:** defined as a rate on inconsistency between transmitted and received packets. Error-rates represent the ratio of successful delivered packets to the unsuccessful or undelivered packets.

Obtaining the above parameters on the active link (marked as primary in an SCTP association) is achievable by monitoring the links and the packet transmission activities. For this purpose on the primary link QoS parameters can be calculated using following methods:

- Monitoring the primary link and counting the number of packet losses during a certain period of time in order to calculate the loss ratio.
- Monitoring the primary link for counting the number of consecutive packet losses in order to predict the possible disconnectivity and handover time.
- Measuring the Round Trip Time (RTT) in order to evaluate the latency and propagation delay.
- Monitoring the size of Congestion Window (cwnd) on the primary link

- Calculating the throughput and the available bandwidth on the primary link using the following formula (7-4):

$$\text{Throughput (or Bandwidth)} = \text{cwnd}/\text{RTT} \quad (7\text{-}4)$$

- Keep track of RTT changes on all available links to monitoring the jitter on each link

As the primary link which is involved in transferring packets from sender to receiver in an SCTP association, monitoring and calculating the QoS parameters are less challenging in comparison with alternative links. To monitor the condition of alternative paths on an SCTP association a dual heartbeat technique proposed in following sections that periodically checks the availability of the paths and monitors the end-to-end delay and available bandwidth.

7.3. Bandwidth Estimation Algorithm for nSCTP

Bandwidth estimation techniques discussed in section 7.1 were designed and developed for the TCP which can handle single home scenarios and they do not have the capability to work in a multi-homed scenarios managed by SCTP or nSCTP. In this section, an extended version of SCTP with built-in feature of bandwidth estimation technique is presented in order to dynamically perform changeover to the most suitable links. Figure 7-2 shows a scenario where in wireless hops three different wireless access network technologies are available. A multi-homed SCTP session between MR-HA and MR is available and the aim is distinguishing a more reliable link based on the QoS parameter (addressed in section 7.2) that helps dynamic switchover on the best available links rather than traditional SCTP failover mechanism.

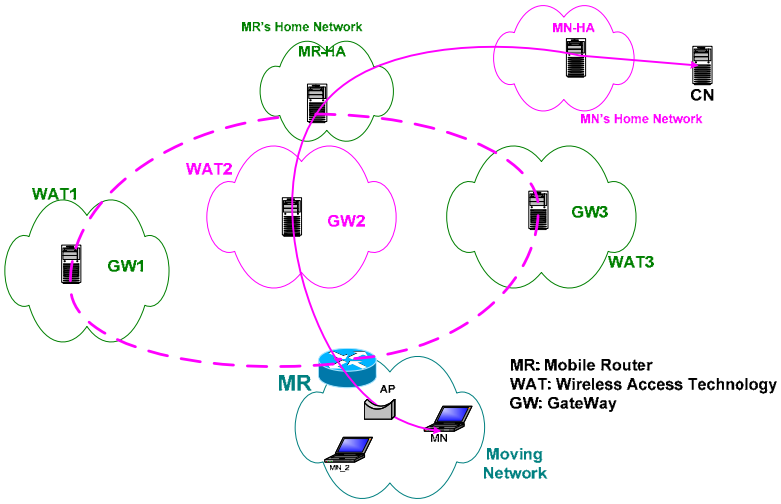

Figure 7-2: Simulation scenario for nSCTP while more than one connection is available

7.3.1. Monitoring the packet loss and the consecutive packet loss

SCTP failover system is based on the number of consecutive packets lost on the primary link. This means that even in a poor communication path, if the number of consecutive packets lost does not exceed a certain predefined threshold, the failover mechanism in SCTP (or handover mechanism in mSCTP and nSCTP) will not be activated. The algorithm presented in this section in addition to monitoring the number of consecutive packet losses is able to calculate the loss ratio (defined in section 7.2) which will result in more accurate changeover mechanism.

The flowchart of this algorithm is shown in Figure 7-3.

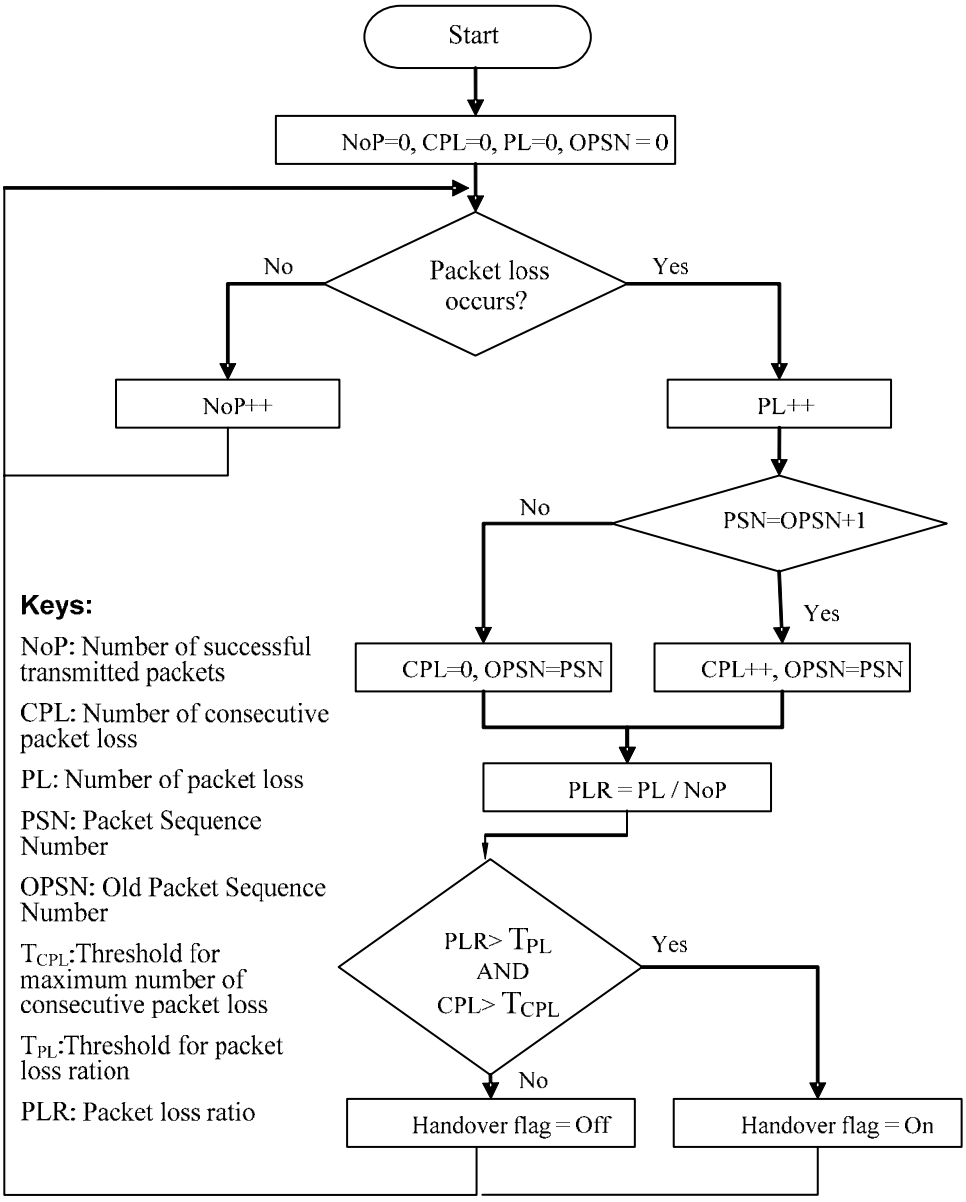

Figure 7-3: handover improvement flowchart based on consecutive and total number of packet loss

7.3.2. Estimating the Available Bandwidth on the Primary link

On the primary link that is considered as a link that carries SCTP chunks, calculating the available bandwidth could be performed either using the techniques explained in section 7.1.2 or monitoring RTT and Window Size as specified in section 7.2 and using the following equation:

$$\text{Bandwidth} = \text{WindowSize} / \text{RTT} \tag{7-5}$$

In order to have a fair estimation of available bandwidth on the primary and the alternative links packet pair technique is used.

7.3.3. Estimating the Available Bandwidth on the Alternative link(s)

Original SCTP uses heartbeat packets in order to periodically check the availability of alternative links. A double heartbeat scenario sending back-to-back is proposed in this chapter. We still assumed that the switching speed and the processing delay of routers are less that transmission delay in the system. The proposed protocol is sender driven which means all the processes such as bandwidth estimation and switching scenarios will be managed by sender side based on received heartbeat-Acks. The system does not need clock synchronisation or any changes on the heartbeat and heartbeat-Ack chunks.

Packet pair technique (see section 7.1.2) is employed to estimate the available bandwidth for the links which are in idle mode in an association between sender and receiver.

$$BW_{Min} = \frac{L}{\Delta T} \tag{7-6}$$

And

$$\Delta T = \Delta T_{out} - \Delta T_{in} \tag{7-7}$$

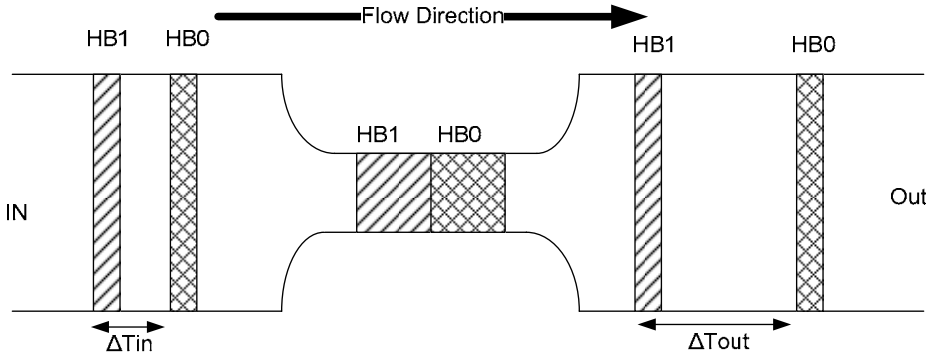

Figure 7-4: Bottleneck link that causes packet queuing when two conscetive heart bit send close enough together

Finding the optimal value for 'ΔT_{in}' is a challenging issue. If the Heartbeat packets are very close to each other ('ΔT_{in}' is small) even in the non-bottlenecked transmission channel they will get queued on the routers when the switching and processing speeds in the routers are not sufficient. Also the value of 'ΔT_{out}' should not be too high as in that case queuing in the bottleneck hop will not increase the input time difference (ΔT_{in}).

The value of 'L' represents the size of the Heartbeat packets. The acceptance range for this size should be large enough to cause queuing and also should not be more than the Maximum Transmission Unit (MTU) to avoid packet fragmentation. MTU sizes are inherent properties of physical network interfaces, normally measured in bytes. The MTU of Ethernet, for instance, is 1500 bytes. Some types of networks (like Token Ring) have larger MTUs, and some types have smaller MTUs, but this value is fixed for each physical technology. Therefore, with the assumption of Ethernet used in physical technology and a packet size of 1500B in the transmission channel and wireless LAN as a bottleneck of the system with the bandwidth of 10Mbps:

$$\Delta T_{Out} = \frac{L}{BW_{Min}} = \frac{1.5KB}{10Mbps} = 1.2ms \tag{7-8}$$

Therefore a value of ΔT_{in}<1.2ms needed to be set at the receiver and similarly with a channel in the range of 2Mbps ΔT_{in} must be less than 6ms.

In the next section a simulation study has been carried out to measure the bandwidth on all available paths within an SCTP association. It is assumed that the switching time of the routers is high enough and will not cause delay when the packets send back-to-back (or ΔT_{in}=0). The value of 'L' is the size of Heartbeat packets in the original SCTP and is equal to 56B which are marked as HB0 and HB1 in Figure 7-4.

7.4. Simulation Studies on Dynamic Switchover Technique within an SCTP Association

To assess the benefit of dynamic switchover extension of SCTP, performance of this proposed protocol is studied using the Network Simulator. As explained in

section 2.5.1, SCTP periodically checks the availability of alternative link(s) by sending Heartbeat signals to the other end in an association. NS-2 network simulator [70] along with SCTP agent [72] developed for NS-2 with some modification for supporting the packet pair scenario have been used as the simulation platform. The following features have been added into original SCTP agent:

- At the beginning of the transmission primary path will be dynamically set by sending a double heartbeat on all available paths and going through the process of choosing the best path.
- At the sender, sending a double heartbeat chunks back-to-back in equal predefined intervals (e.g. 15 seconds as default value). The interval time may set at the beginning of simulation as it may vary for different applications and network conditions.
- At the receiver, both received heartbeat will be acknowledged. This is part of the original feature of SCTP and no modification has been done.
- At the sender, available bandwidth will be calculated based on the time difference on the received acknowledgement (ΔT_{out}).
- Based on the estimated bandwidth on all available paths, at particular intervals the most appropriate path will be selected as a primary link for the SCTP association. This allows the end users to dynamically decide about the best connection.

7.4.1. Simulation Scenario

In any data transmission system, one of the most important parameters from a user's point of view is the amount of data transmitted during a certain time, which is identified as connection throughput. If dynamic path selection could configure the primary connection on the best available bandwidth, the transmission rate could be improved. However, some parameters like signalling and processing overhead used for detecting the best available bandwidth on the paths will reduce the overall performance of the dynamic path selection scheme.

Figure 7-5 depicts the implemented scenario in NS-2 consisting of air interface connection with different wireless access technologies and different available bandwidth. As the MR moves the signal strength of the wireless connection will be changed and with respect to Shannon's formula [5] the signal to noise ratio will be reduced and consequently the available bit-rate will decrease. In addition to the movements of MR, available bandwidth will be changed based on the traffic applied to the network from all other users connected to this network.

The developed scenario in the simulation platform (NS-2) is shown in Figure 7-5. All the connections outside the wireless part of the connection have sufficient bandwidth (100Mbps) and the bottleneck part of the network is on the wireless hop(s) between MR's Home agent and its peer MR. There are four paths available that their throughput will be changed during the simulation time between 1 to 11 Mbps in order to form a non-structural changes on the link capacity.

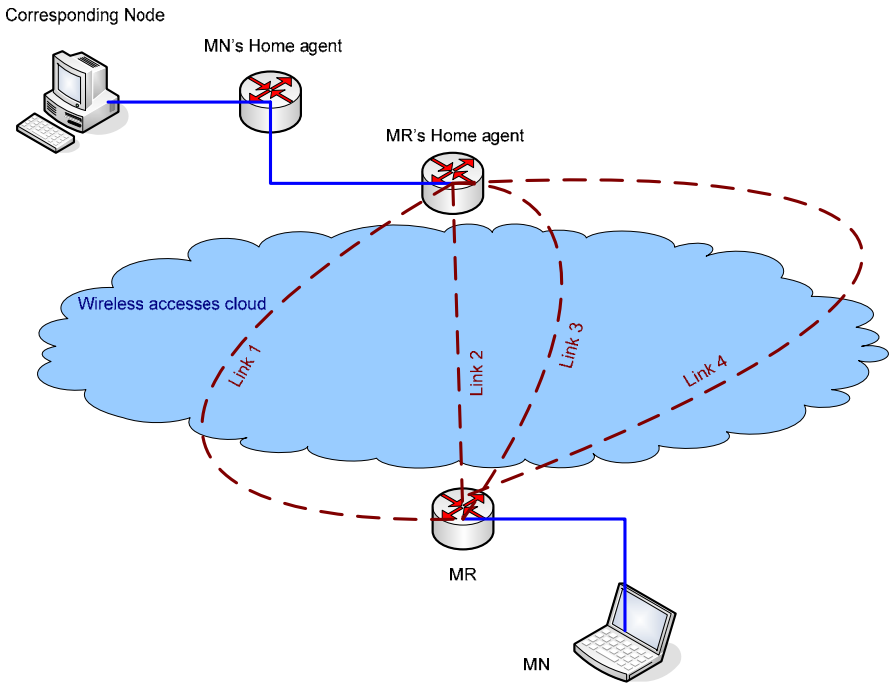

Figure 7-5: Dynamic handover mechanism topology based on nSCTP implemented in NS-2

The Double Heartbeats module has been added to the current implemented version of SCTP [72] for sending two probing packets back-to-back in the certain

intervals. The size of probing packets are 56kB, similar to the size of heartbeat packet in the original SCTP, and the interval time for sending the probing packets has been set to 5 seconds. The interval time could be varying based on the network condition and the requirement of the network. Choosing small value for interval time for sending packet will result in a switchover upon a link bandwidth has changed however it will increase the signalling on the network.

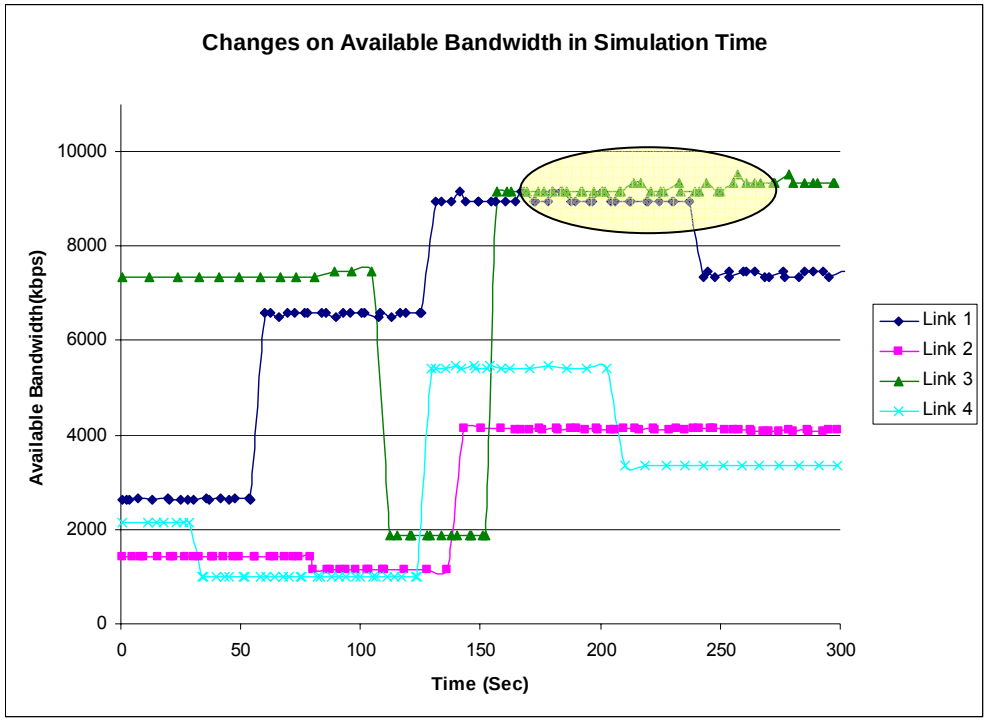

Figure 7-6: Bandwidth response acquired from the available link in the wireless cloud in Figure 7-5

Figure 7-6 shows the output of packet pair modules, which follows the available bandwidth on all links within an SCTP association. In the original SCTP protocol, the primary link will not change until it becomes unavailable or certain amount of consecutive packet lost (usually three) is detected. At the beginning of the simulation link 1 has been chosen for primary link.

Goodput is the amount of useful data which has been acknowledged successfully. For analysing the performance of new QoS scheme, two scenarios were defined based on the result simulation presented in Figure 7-6. At the first scenario, the changeover policy on the SCTP association is set to be static as it is defined in

the original protocol. Therefore, as there is no consecutive packet loss or disconnectivity due to the handover, link1 will remain the primary link and goodput for this simulation is shown in Figure 7-7.

In the second scenario, the primary link will follow the highest bandwidth on the available links. The available bandwidths on all links check periodically (in this simulation every 5 seconds) and upon the extension of SCTP association detects a higher bandwidth path the primary link will be changed to that particular path and the transmission will be resumed. The primary path for this scenario is shown on Figure 7-7 for better comparison with static changeover scenario. This clearly shows that the dynamic changeover scenario has better goodput performance compared to the original static failover in SCTP.

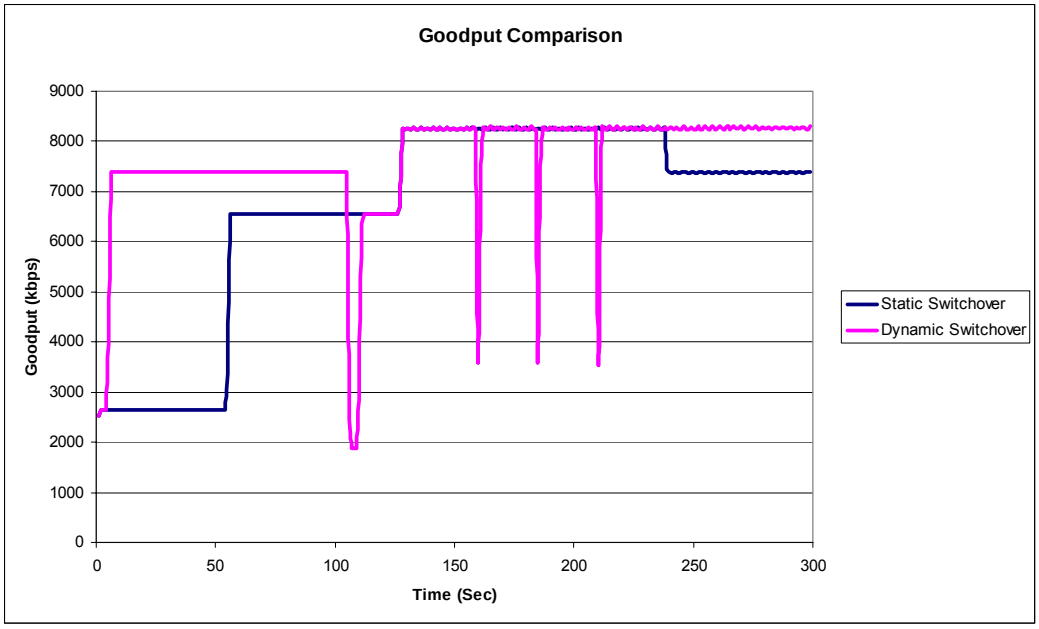

Figure 7-7: Goodput comparison of two schemes - original SCTP and SCTP with dynamic changeover mechanism

7.4.2. Enhanced Dynamic switchover mechanism

Figure 7-7 shows the improvement of throughput compared to the original version of SCTP. SCTP slow start and congestion avoidance mechanism caused the sudden reduction of the received goodput as shown in Figure 7-7. Some other improvements could be applied to overcome this problem and increase the performance of this new scheme.

Firstly, at the beginning of the transmission on the static handover scenario the SCTP association automatically chooses the primary link and after receiving the results of the first sets of probing signals the SCTP association will select the highest available bandwidth. This will cause an unnecessary handover at the beginning of the transmission. This issue is shown clearly in Figure 7-8. The above problem can be solved by sending the probing packet pair at the beginning of transmission and choosing the primary connection before performing the four ways handshakes and starting packet transmission.

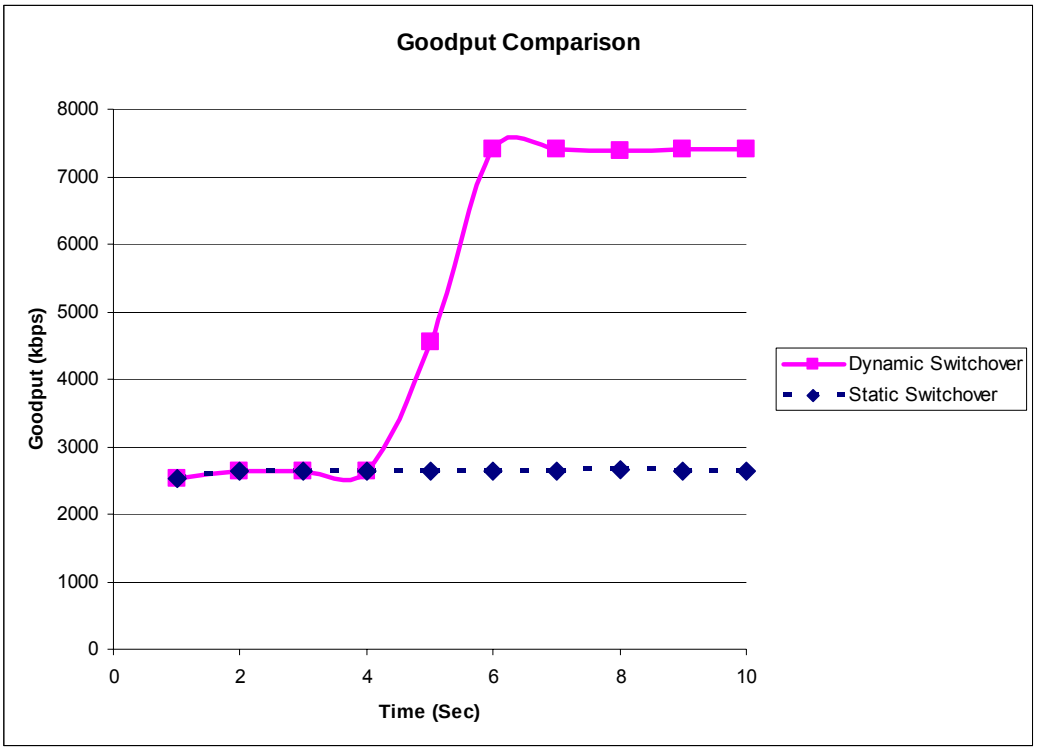

Figure 7-8: the problem of starting at a low bandwidth link and then switch to the higher bandwidth

The second enhancement is aimed at increasing the throughput and reducing the unnecessary handovers where possible. Frequently handover for small differences on available bandwidth could significantly reduce the performance of this new proposed scheme. This reduction is due to the slow start and congestion avoidance procedures as shown in Figure 7-9. This issue fully reflected in the Figure 7-7 between times 160 to 230 seconds as the bandwidth on links 3 and 5 fluctuating in a small difference on the highlighted region in Figure 7-6.

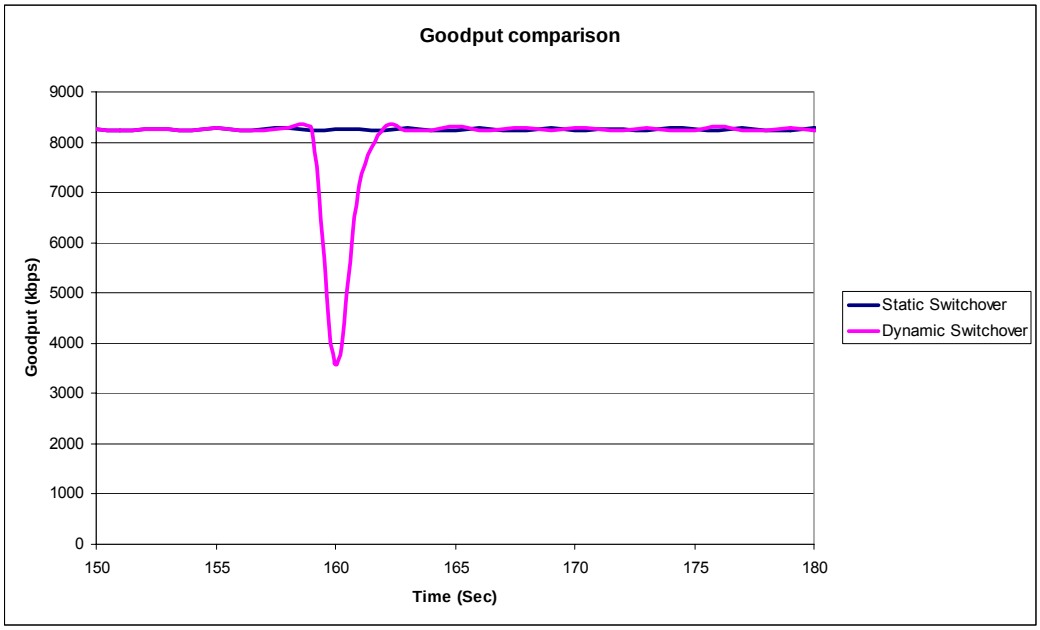

Figure 7-9: the problem of slow start of SCTP while a handover is performing

The goodput of improved version of this protocol is shown in Figure 7-10 while a 10% threshold for switchover has been defined. A massive improvement compared to static failover mechanism could be observed. Also, compared to the previous scenario, stability has been improved as well as the overall throughput has been increased. A comparison of total packet transferred during the simulation time is presented in Table 7-1 and the trend of the received packet's aggregation is shown in Figure 7-11.

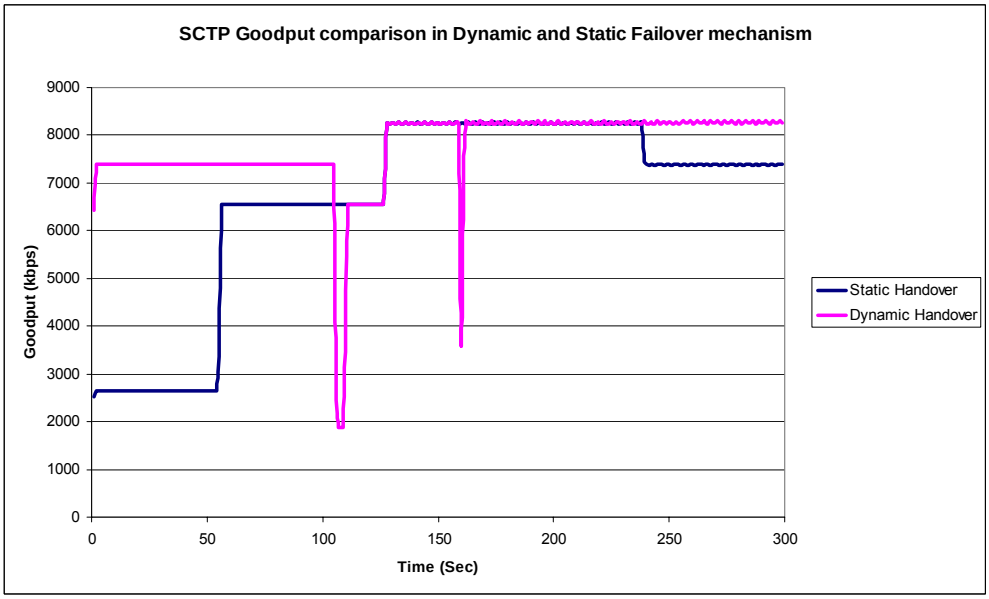

Figure 7-10: Goodput comparison in Static and Dynamic handover scenarios

	Static Handover	Dynamic Handover	Enhanced Dynamic Handover
Total received packet at the receiver	168,828 Packets	190,532 Packets	193,354 Packets

Table 7-1: Total received packet during the simulation time with different handover schemes

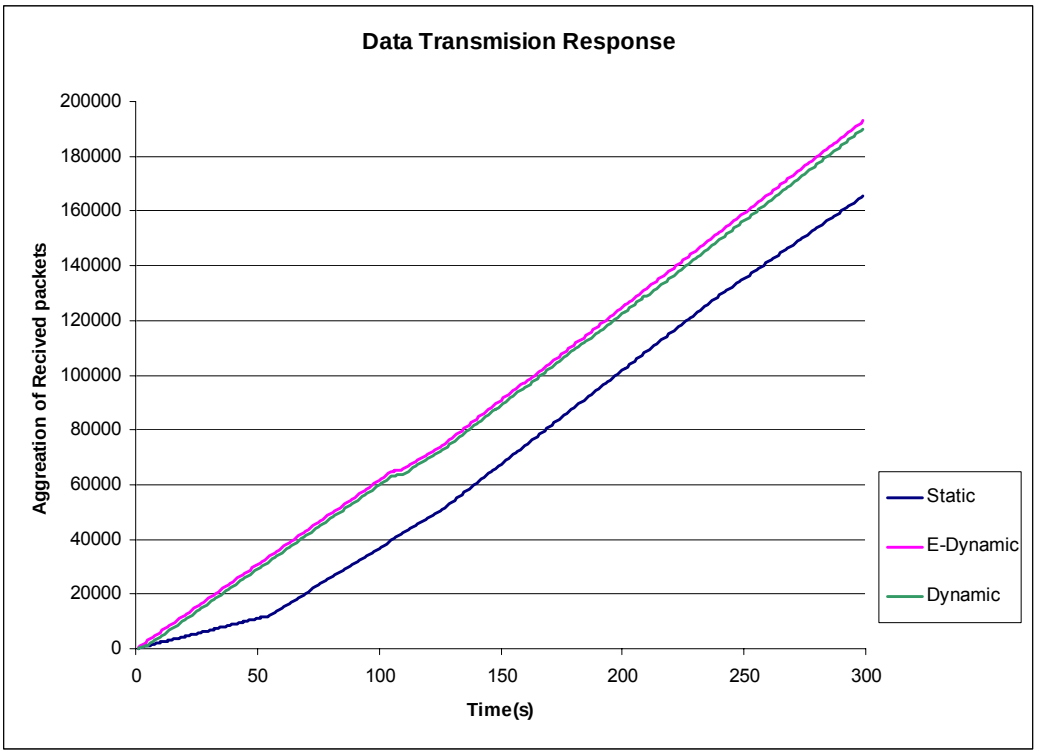

Figure 7-11: Aggregation of received packet on different switching over techniques (Static, Dynamic and Enhanced Dynamic handover)

7.5. Results Comparison and Discussion

Defining a suitable switchover time for dynamic handover scenario, proposed in this chapter, is a challenging issue. On one side, increasing in the number of handover is one of undesirable parameters that in some applications must be avoided and on the other side, sticking to a link while some more efficient links

are available decreases the amount of transferred packet in time unit. A switching over threshold was defined in section 7.3. In this section the amounts of received packets and the number of handovers while the switching over threshold is changing are compared.

For the analysis, three different triggering rules which specified the appropriated time for switchover are defined as follows:

- Aggressive: Switchover when a link with higher bandwidth has been detected.
- Conservative: Switchover when the new detected bandwidth is above a certain threshold.
- Sluggish: The primary link will not be changed to the highest available link while the transmission can still performed on the current active link.

The performances of proposed QoS provisioning for SCTP have been experimented through the implemented simulation in NS-2 platform (detail of simulation topology presented in section 7.4) and the results of aggregated received data is shown in Figure 7-12. Four different scenarios including aggressive, conservative with threshold of 10% and 25% and sluggish are evaluated. Links 1 to 4 shown in Figure 7-5 fluctuating between 1 and 11 Mbps. The results show that the aggregation of the received data is maximised in the case of aggressive scenario and will be reduced by decreasing the threshold in conservative scenarios and finally the less effective amount of transferred data has been allocated to sluggish scenario.

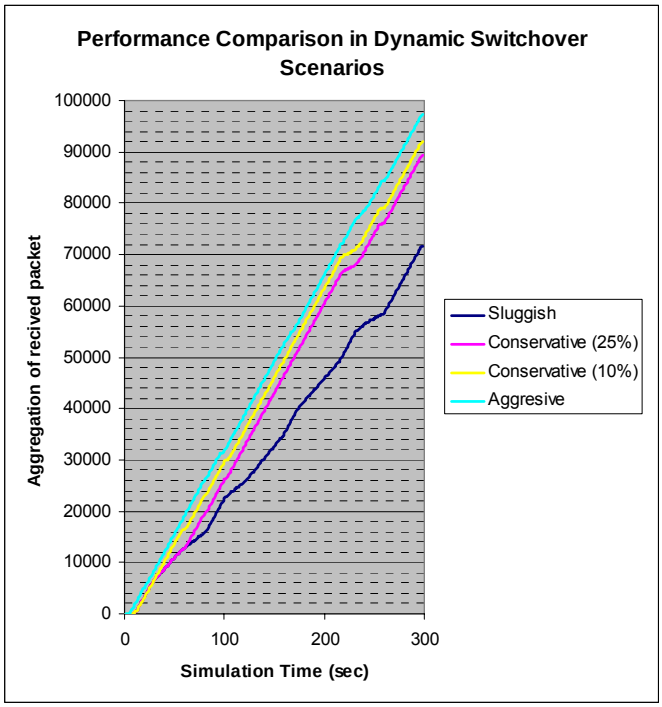

Figure 7-12: Performance comparison in dynamic switchover in aggressive, conservative and sluggish scenarios

The penalty of achieving the maximum transmitted data depicted in Figure 7-12 is increasing the number of handovers for small fluctuation between available links within an SCTP association. While the proposed handover protocol in this thesis (nSCTP) is seamless but during the handover a reduction of services due to slow start and congestion avoidance of reliable transport layer protocols for a short time can be observed (see Figure 7-7). By analysing the number of handovers, aggregation of transferred data and the value of threshold in one experiment the optimal value based on the usage and application could be specified. Two bandwidth scenarios were studied based on the simulation scenario presented in Figure 7-5. In the first scenario the available bandwidth allocated to the links 1 to 4 fluctuating within 1 to 2 Mbps. Based on the result is shown in Figure 7-13 when the switchover threshold is about 0 percent the maximum number of handovers is experienced and the highest aggregation of data is achievable. While the switchover policy moves to conservative scenarios with different thresholds the number of handovers decreases and consequently the transferred packet rate will be decreased. This obviously is not always true e.g. between 35 to 40 percent packet transferred is decreases which is the effect of unnecessary switchover, which was discussed in section 7.4.2. The result for a similar experience with high bandwidth is shown in Figure 7-14. In this

scenario the link bandwidths changes between 1 to 11Mbps and similar result of indirect relation between threshold of switchover and number of handover or number of transferred packets can be observed.

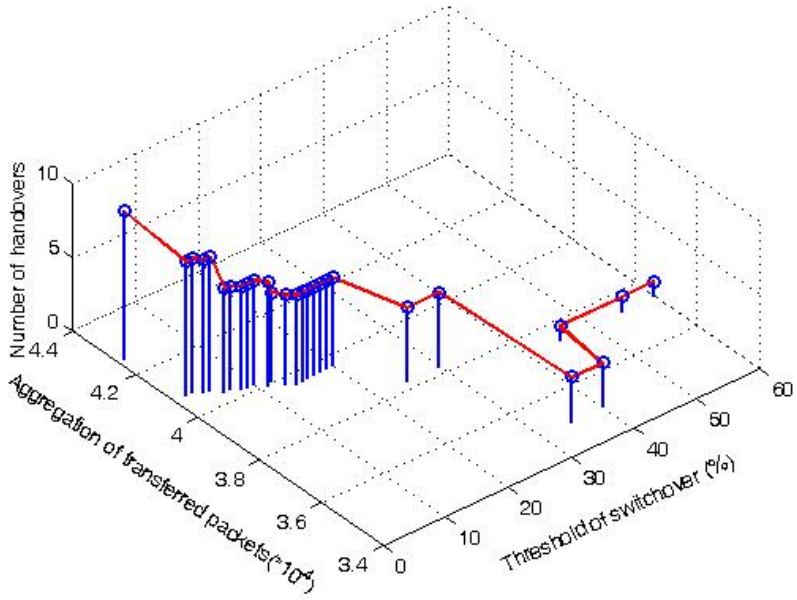

Figure 7-13: The impact of threshold switchover on the amount of transferred data and the number of handovers in low bandwidth scenarios

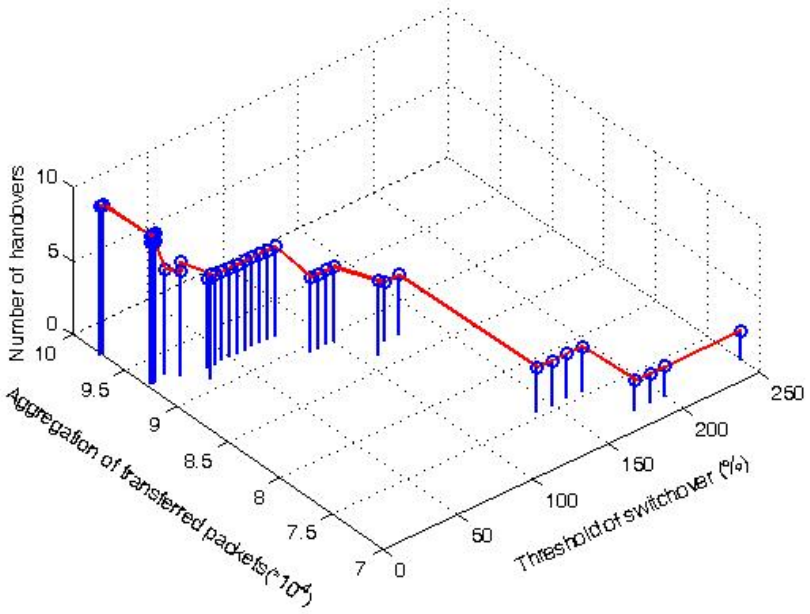

Figure 7-14: The impact of threshold switchover on the amount of transferred data and the number of handover in high bandwidth scenarios

7.6. Chapter Summary

In this chapter a dynamic switchover scheme for improving the QoS of SCTP and nSCTP particularly when variety range of wireless access networks are available is proposed. Efficiency of this protocol in reducing the packet loss by shrinking the handover latency and increasing the end-to-end throughput in wireless access has been considered. It has been shown that the new QoS scheme could significantly increase the throughput particularly when the available bandwidths on the primary and alternative links change frequently due to movement and/or congestion.

Chapter 8. Conclusion

The scope for mobile networks to be multi-homed is certain to be a significant aspect of future communications systems. This multi-homing capability is being continually extended through the progressive migration of a single mobile node to an entire network. Multiple links in the chain of multi-homing will be used to provide redundancy in connections, and therefore achieve a soft and seamless handover or in the other words guarantee a QoS threshold for a moving network. This thesis has thus investigated a number of solutions to assist mobile networks multi-homing feature, and has particularly concentrated on mobility management issues as might apply in a scenario such as mass public transportation in a train or coach.

In this thesis, different mobility management from different layers of OSI reference model in a heterogeneous environment were compared, their advantages and disadvantages to handle the mobility in different layers were mentioned and the weaknesses of Mobile IP as a mobility management protocol were described. Internet connectivity for moving networks in a wired-cum-wireless scenario in a heterogeneous environment and different aspects of multi-homing for mobile networks were characterised. Multi-homing for moving networks is the next part of overview of this thesis that can enhances QoS parameters and especially facilitating a seamless handover.

The main contribution of this thesis was proposing useful solutions to improve the performance of handover for mobile networks. nSCTP as a new mobility management protocol to achieve a seamless handover for moving networks has been proposed. This protocol works based on SCTP which allows binding of one transport layer association to multiple IP addresses at each end of the association. SCTP has a built-in failure detection and recovery system, known as failover, which allows associations to dynamically send traffic to an alternate peer IP address when needed.

To evaluate the performance of nSCTP, this thesis has developed simulation based studies for comparing the different extensions of TCP with the recently proposed transport level protocol, SCTP, to compare them in a combined wired-

wireless scenario in a cellular network with vertical handover. The major achievements here have been the investigation of congestion window, handover delay and throughput for download file sizes in general, and the study through simulation for multi-homing scenarios over a bottleneck link, which is the wireless part of the network for a single mobile node or the connection between mobile router and its home agent for a moving network.

We have evaluated NEMO and nSCTP analytically in terms of three main handover parameters; packet loss, handover delay and throughput. The results of numerical examples of this model show that some significant improvements can be achieved by using nSCTP. A parallel simulation based analysis has been done in which results show that soft handover in heterogeneous networks can be achieved for a mobile network and the performance and robustness of connection is much higher than NEMO.

Using developed protocol, not only providing a fully soft and seamless handover; it can also improve reliability in the bottleneck of the network (MR to MR-HA) with the cost of increasing the size of packet overhead. The wireless part of network is generally involved with higher bit error-rate, but in this scheme packet lost can be solved locally without involving the rest of the network. End user transparencies, no dis-connectivity and no changes in the Internet architecture are some of the main advantages of nSCTP.

Improving the QoS parameters such as reducing the handover latency and packet loss during the handover and increasing the overall throughput of the system were another contribution of this thesis. Failover mechanism of original SCTP is static and will not be adapted to the condition of the network and available paths. A dynamic switchover scheme for SCTP and nSCTP is proposed in this thesis that monitors the available bandwidth on the associated paths within a multi-homed association. This scheme is advantageous particularly when variety ranges of wireless access networks are available. Efficiency of this protocol in reducing the packet loss by shrinking the handover latency and increasing the end-to-end throughput in wireless access has been considered by a developed simulation in the NS-2 platform. It has been shown that the new QoS scheme could perform extremely well, when different choices of paths exist and the

available bandwidths on the primary and the alternative links change frequently due to movement and/or congestion.

Applicability of the proposed protocol is provided in the following section and it has been followed by potential for future work. The security and billing issues, which are important subjects from a provider's point of view, have not been addressed in this thesis. Load balancing and load sharing are other open issues of this protocol that can significantly improve the performance of SCTP and nSCTP.

8.1. Applicability of the Solutions Provided

The solutions presented in this thesis serve the primary objective of improving the effectiveness and applicability of mobility management for moving networks. Moreover, they are developed to be as feasible as possible in generic systems either through being targeted at simple all-IP networks, or otherwise through requiring minimal changes to existing technologies where necessary. Only upgrading to routers at mobile networks (MR) and its home agent (MR's HA) to support transport layer protocols and also minor software changes at these routers' operating systems to load SCTP/IP encapsulation modules are necessary to achieve the solutions presented.

The monitoring scheme presented for improving the QoS provisioning for moving networks could be easily integrated with current version of SCTP. Firstly, the proposed QoS scheme is sender side that no additional to cellular systems or the destination nodes are required. Secondly, different policies based on the users' requirements are achievable to increase the flexibility of the system and improve users' satisfaction.

8.2. Potential for Future Work

Substantial potential for future work has been created through the many avenues investigated in this thesis.

Firstly, in the context of the SCTP, multi-streaming which is the main feature of this protocol, has not involved in the investigation. This feature can potentially can be used to put emphasise on different application by defining dissimilar values for each streams and multiple priority policy for incoming packets. This policy based scenario can guarantee for handling the realtime or time sensitive programs before other applications.

Secondly, in the context of the nSCTP, proposed as a handover management protocol for moving networks was presented completely and all the possible algorithms and transport layer tunnelling were discussed in this thesis. This is a very new protocol with a full theoretical, analytical and simulation support, but further investigation could be addressed and lots of work can be done in order to improve the throughput by improving the tunnels and reducing overhead. In this context the following issues can be addressed for future investigations:

- Multi-homing has built in load sharing and load balancing techniques, which at the present time are not supported by SCTP and consequently nSCTP. Load sharing refers to splitting the traffic from a network to be transported and load balancing is distributing the traffic dynamically among available paths to avoid congestion and saturation. Bandwidth aggregation is an on demand issue specially by growing up the volume of data and different applications that can be observed on the Internet. A newly proposed IETF draft [37] considered multiple CoA for multiple interfaces mobile nodes that has been used in [84] for load balancing based on SCTP. Activating load balancing and sharing with nSCTP can significantly improve the performance of this protocol. For nSCTP and the architecture that we concentrated on this thesis MR and MR-HA are the best options for handling load balancing.
- Multi-homing will certainly be the most important issue in the mobility management in the coming years. With the recent deployment of different wireless technologies and the new version of the IP protocol, almost all nodes will be multi-homed. Therefore, nested mobile network and adaptation of nSCTP for these sorts of moving networks, is an interesting area that could be investigated.

Some interesting avenues for future works are research on the transport layer tunnelling algorithms and nSCTP that can be addressed as follow:

- QoS is an important issue in the current and future world of computer networks. nSCTP can improve some QoS parameters like handover delay, packet loss and throughput but all of these improvements are subject to availability of resources in the visiting cells. Advance resource reservation for hire resources before moving is a vital issue especially for a group of mobile nodes which roams together. This can provide a guaranteed QoS threshold for blocking probability. Also interesting is to study the behaviour of various QoS division policies in the context of advance resource reservation before the MR moves to the new coverage area. Resource reSerVation Protocol (RSVP) [85] is an IntServ-style Quality of Service (QoS) protocol that allows channels and paths to be reserved for both unicast and multicast transmission. RSVP in the similar way of SCTP sends periodic refresh messages to maintain its state and reservation will be deleted in the absence of refresh messages. Conventional RSVP is designed for fixed networks, and there have been a number of extensions on supporting the QoS in Mobile environment with RSVP [86]. Adapting this protocol for mobile networks solutions along with nSCTP apparently can reduce the blocking probability.
- DVB-H recently has been gaining more interest in the research community and with mobile network providers and users as it can enable broadcast services in public transport or the next generation of moving networks. As DVB-H is a uni-directional access network (down-link only), using a bi-directional access network, such as UMTS and/or WLAN, is necessary to be used in conjunction with DVB-H. As a result, MR using the facility of DVB-H access network should have at least two interfaces (one for DVB-H and another one for UMTS/ WALN). Therefore, any possible solution for this scenario must provide multi-homing and nSCTP protocol can be a very good nominate.

Publications Resulting from this Thesis

The following works have been published as a result of this thesis. They are listed in chronological order.

Conferences:

[1] **P. Behbahani**, N. Nafisi and A.H. Aghvami, "A New RSVP Path Management for Mobile Internet," EPSRC, *IEEE, IEE, Postgraduate Research Conference in Electronics, Photonics, Communications and Networks, and Computing Science (PREP 2005),* University of Lancaster, Lancaster UK, March 2005.

[2] A Roos, N Bayer, D Sivchenko, **P Behbahani**, et al., "Broadband Wireless Internet Access in Public Transportation," *Proceedings of the VDE congress Innovations for Europe* , Aachen, Germany, October 2006.

[3] **P Behbahani**, V Rakocevic and J Habermann, "nSCTP: A New Transport Layer Tunnelling Approach to Provide Seamless Handover for Moving Networks," *Proceeding of IFIP/IEEE International Conference on Mobile and Wireless Communications Networks(MWCN' 07),* Cork, Ireland, September 2007

[4] **P. Behbahani**, V. Rakocevic and J. Habermann, "Throughput Enhancement in Heterogeneous Mobile Networks using nSCTP," *Proceeding of IEEE Vehicular Technology Conference 2008 (VTC' 08Fall),* Calgary, Canada, September 2008

Technical Reports:

[5] **P. Behbahani** and V. Rakocevic, "Connection Robustness for Fast Moving Networks in Cellular Networks Using Transport Layer Multihoming," BIT Annual Technical Report, WP5, April 2006.

[6] **P. Behbahani** and V. Rakocevic, "nSCTP: A New Handover Protocol To Providing Connection Robustness for Fast Moving Networks in Cellular Networks Using Transport Layer Multi-homing, " BIT Annual Technical Report, WP5, May 2007.

References:

[1] C. Perkins, "IP Mobility Support for IPv4," *IETF RFC 3344*, August 2002.

[2] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol," *RFC 3963*, January 2005.

[3] R. Stewart, et al., "Stream Control Transmission Protocol," in *RFC 2960, Network Working Group*, October 2000.

[4] A. S. *Tanenbaum*, *Computer Networks*, 4th Ed. ed: Prentice- Hall, 2003.

[5] C. E. Shannon, "A mathematical theory of communications," *Bell System Technical Journal*, Jan. 1948.

[6] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," *RFC 3775*, June 2004.

[7] R. Stewart, M. Ramalho, Q. Xie, M. Tuexen, and P. Conrad, "Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration," IETF RFC 5061, September 2007.

[8] S. J. Koh and Q. Xie, "mSCTP with Mobile IP for Transport Layer Mobility," in *Internet draft version 3. IETF*, February 2004.

[9] P. Behbahani, V. Rakocevic, and J. Habermann, "Throughput Enhancement in Heterogeneous Mobile Networks using nSCTP," presented at Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th, Calgary, Canada, Sep. 2008.

[10] W. M. Eddy, "At What Layer Does Mobility Belong?" *Ieee Communications Magazine*, vol. 42, pp. 155-159, 2004.

[11] M. Ratola, "Which Layer for Mobility? - Comparing Mobile IPv6, HIP and SCTP," Helsinki University of Technolog, Telecommunications Software and Multimedia Laboratory 2004.

[12] M. Atiquzzaman and A. S. Reaz, "Survey and Classification of Transport Layer Mobility Management Schemes," *PIMRC*, 2005.

[13] H. Kaaranen, A. Ahtiainen, L. Laitinen, S. K. Naghian, and V. Niemi, *UMTS Networks Architecture, Mobility and Services*, vol. 1, 2nd ed: John Wiley & Sons Ltd, 2005.

[14] H. Kaaranen and A. Ahtiainen, *UMTS Networks*: John Willey & Sons, New York, 2001.

[15] ETSI, "European Telecommunications Standards Institute (ETSI), http://www.etsi.org/."

[16] L. Harte, *Introduction to 802.11 Wireless LAN (WLAN): Technology, Market, Operation, Profiles, & Services*: ALTHOS, 2004.

[17] Wirelessman.org, "IEEE 802.11 Standard - 2007."

[18] Wirelessman.org, "IEEE 802.16 Task Group 1 <http://wirelessman.org/tg1/>."

[19] H. Soliman, C. Castelluccia, K. El-Maki, and L. Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)," in *IETF RFC 4140*, August 2005.

[20] S. J. Koh, M. J. Chang, and M. Lee, "mSCTP for Soft Handover in Transport Layer," *IEEE Communications Letters*, vol. 8, pp. 189-191, 2004.

[21] M. Riegel and M. Tuexen, "Mobile SCTP," in *IETF Internet Draft, draft-riegel-tuexen-mobile-sctp-09.txt*, Nov. 2007.

[22] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: Session Initiation Protocol." IETF RFC 3261, 2002.

[23] P. Behbahani and V. Rakocevic, "Connection Robustness for Fast Moving Networks in Cellular Networks Using Transport Layer Multihoming," *BIT Annual Technical Report, WP5*, April, 2006.

[24] R. Shacham, H. Schulzrinne, S. Thakolsri, and W. Kellerer, "Session Initiation Protocol (SIP) Session Mobility," *IETF RFC 5631*, October 2009.

[25] W. A. Romijn, D. Plas, D.Bijwaard, E. Meeuwissen, and G. Ooijen, "Mobility management for SIP sessions in a heterogeneous network environment," *Bell Labs Technical Journal*, 2004.

[26] R. Stewart, M. Ramalho, Q. Xie, M. Tuexen, and P. Conrad, "Stream Control Transmission Protocol (SCTP) Partial Reliability Extension," *IETF RFC 3758*, MAY 2004.

[27] R. Stewart and P. D. Amer, "Why is SCTP needed given TCP and UDP are widely available?" http://www.isoc.org/briefings/017/, Sep. 2007.

[28] C. Perkins, "IP Mobility Support," *IETF RFC 2002*, Oct. 1996.

[29] C. Perkins, "IP Encapsulation within IP," *IETF RFC 2003*, October 1996.

[30] E. T. Melia, G. Bajko, S. Das, N. Golmie, and J. Zuniga, "IEEE 802.21 Mobility Services Framework Design (MSFD)," *IETF RFC5677*, Dec. 2009.

[31] M. Nicolas, N. Thomas, and E. Thierry, *Multihoming in Nested Mobile Networking*: IEEE Computer Society, 2004.

[32] R. Moskowitz, "Host Identity Payload and Protocol," in *Internet draft, version 5, IETF*, October 2001.

[33] P. Nikander, T. Henderson, C. Vogt, and J. Arkko, "End-Host Mobility and Multihoming with the Host Identity Protocol," IETF RFC 5206, April 2008.

[34] S. Novaczki, L. Bokor, and S. Imre, "A HIP Based Network Mobility Protocol," presented at SAINT Workshops 2007, Jan 2007.

[35] H.-Y. Hsieh and R. Sivakumar, "A Transport Layer Approach for Achieving Aggregate Bandwidths On Multi-homed Mobile Hosts," presented at ACM Mobicom '02, 2002.

[36] A. Habib, N. Christin, and J. Chuang, "Taking Advantage of Multihoming with Session Layer Striping," presented at INFOCOM 2006, April 2006.

[37] R. Wakikawa, T. Ernst, K. Nagami, and V. Devarapalli, "Multiple Care-of Addresses Registration," in *draft-ietf-monami6-multiplecoa-02.txt*, May 2007.

[38] M. Mahamat-Faki and J.-M. Bonnin, "Bringing multi-tunneling management to Ubique framework," *ITS Telecommunications Proceedings, 2006 6th International Conference*, June 2006.

[39] Y. Choi, B. Kim, S.-H. Kim, M. In, and S. Lee, "A Multihoming Mechanism to Support Network Mobility in Next Generation Networks," Aug 2006.

[40] M. A. Rónai and e. al, "Concept of Mobile Router and Dynamic IVAN Management," *IST-2001-35125 (OverDRiVE) D07*, 2003.

[41] H. Lach, C. Janneteau, and A. Petrescue, "Network Mobility in Beyond-3G Systems," in *IEEE Communications Magazine, pages 52-57*, July 2003.

[42] T. Ernest, "Network Mobility Support Goals and Requirements," July 2007.

[43] T. Ernst, A. Olivereau, and H. Lach, "Mobile Networks Support in Mobile IPv6 (Prefix Scope Binding Updates)," in *IETF Internet Draft, draft-ernst-mobileip-v6-network-02.txt*, 2002.

[44] T. J. Kniveton, J. Malinen, V. Devarapalli, and C. E. Perkins, "Mobile Router Tunneling Protocol," IETF draft-kniveton-mobrtr-03.txt, November 2002.

[45] R. Wakikawa, S. Koshiba, K. Uehara, and J. Murai, "ORC: Optimized Route Cache Management Protocol for Network Mobility," In Proceedings of the 10th IEEE International Conference on Telecommunications, ICT 2003, Papeete, Tahiti, February 2003.

[46] OpenSSH, "OpenSSH, http://www.openssh.com/."

[47] vtun, "Virtual Tunnels over TCP/IP networks, http://vtun.sourceforge.net/."

[48] HTUN, "HTTP Tunnelling Interface, http://htun.runslinux.net/."

[49] O. Titz, "Why TCP over TCP is a bad idea," http://sites.inka.de/sites/bigred/devel/tcp-tcp.html, 2001.

[50] S. Floyd and K. Fall, "Promoting the Use of End-to-End Congestion Control in the Internet," *IEEE/ACM Transactions on Networking*, August 1999.

[51] C. Ng, T. Ernst, E. Paik, and M. Bagnulo, "Analysis of Multi-homing in Network Mobility Support," *RFC 4980*, October 2007.

[52] P. Savola, "MTU and Fragmentation Issues with In-the-Network Tunneling," *IETF RFC 4459*, April 2006.

[53] J. Postel, "Internet Protocol," September 1981.

[54] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," *IETF RFC 2460*, Dec. 1998.

[55] C. Fraleigh, S. Moon, B. Lyles, C. Cotton, M. Khan, D. Moll, R. Rockell, T. Seely, and C. Diot, "Packet-Level Traffic Measurements from the Sprint IP Backbone," *IEEE Network*, vol. 17, pp. 6-16, 2003.

[56] I. Aydin, W. Seok, and C. C. Shen, "Cellular SCTP: A Transport-Layer Approach to Internet Mobility," presented at International conference on computer communications and networks; ICCCN 2003, Dallas, TX, 2003.

[57] M. Jacobson, O. Nordstrom, and R. J. Clark, "HTun: Providing IP service over an HTTP proxy," in *http://htun.runslinux.net/docs/htun-paper.pdf*.

[58] B. P. Lee, R. K. Balan, L. Jacob, W. K. G. Seah, and A. L. Ananda, "TCP tunnels: avoiding congestion collapse," in *Local Computer Networks, LCN 2000. Proceedings. 25th Annual IEEE Conference on*, 2000.

[59] H. T. Kung and S. Y. Wang, "TCP Trunking: Design, Implementation and Performance," presented at Proceedings of the Seventh Annual International Conference on Network Protoco, 1999.

[60] S. Fu and M. Atiquzzaman, "Performance Modeling of SCTP Multihoming," in *IEEE GLOBECOM Proceeding*, 2005.

[61] L. Ma, F. Yu, and V. C. M. Leung, "Modeling SCTP Throughput in Integrated WLAN/Cellular Networks," *Proc. IEEE ICC05*, May 2005.

[62] W. Stevens, "TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms," in *IETF RFC2001*, Jan 1997.

[63] J. Padhye, V. Firoiu, D. Towsley, and J. Krusoe, "Modeling TCP Throughput: A Simple Model and its Empirical Validation," *Proceedings of the ACM SIGCOMM '98 conference on Applications, technologies*, 1998.

[64] Z. YI, T. SAADAWI, and M. LEE., "Analytic model of Stream Control Transmission Protocol.," presented at Proc. International Workshop on Performance Modelling of Computer Communication Systems (PMCCS), Monticello, Illinois, USA, Sep. 2003.

[65] V. Basto and V. Freitas, "SCTP Extensions for Time Sensitive Traffic," presented at International Network Conference (INC 2005), Doryssa Bay Resort, Samos Island, Greece, 2005.

[66] J. Kurose and K. Ross, *Computer Networking - A Top-Down Approach*: Addison Wesley, 2008.

[67] S. Floyd, T. Henderson, and A. Gurtov, "The NewReno Modification to TCP's Fast Recovery Algorithm," in *RFC3782*, April 2004.

[68] M. Mathis, J. Mahdavi, S. Floyd, and A. Romanow, "TCP Selective Acknowledgment Options," *RFC 2018*, October 1996.

[69] M. Allman, V. Paxson, and W. Stevens, "TCP Congestion Control," *IETF RFC2581*, Apr. 1999.

[70] NS-2, "The Network Simulator - ns-2, <http://www.isi.edu/nsnam/ns/>."

[71] M. C. Jae Chund, "NS By Example <http://nile.wpi.edu/NS/>."

[72] PEL, "Protocol Engineering Lab, University of Delaware, http://pel.cis.udel.edu/."

[73] "The Open Group Base Specifications Issue 6 IEEE Std 1003.1<http://www.opengroup.org/onlinepubs/000095399/utilities/awk.html>."

[74] E. Hyytiä and J. Virtamo, "Random Waypoint Mobility Model in Cellular Networks <http://www.netlab.hut.fi/u/esa/>."

[75] G. Lin, G. Noubir, and R. Rajaraman, "Mobility models for ad hoc network simulation," presented at Proceedings of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM ⁄04), vol. 1, pp. 454-463, Hongkong, March 2004.

[76] S. Bellovin, "A Best-Case Network Performance Model," *Tech. Rep*, Feb. 1992.

[77] V. Jacobson, "Pathchar: A Tool to Infer Characteristics of Internet Paths," Apr. 1997.

[78] K. Lai and M. Baker, "Measuring Link Bandwidth Using a Deterministic Model o Packet Delay," presented at ACM SIGCOMM, Sep. 2000.

[79] K. Lai and M. Baker, "Nettimer: A Tool for Measuring Bottleneck Link Bandwidth," presented at USENIX symposium on Internet technologies and systems, San Francisco, CA, 2001.

[80] J. C. Bolot, "End-to-End Packet Delay and Loss Behavior in the Internet," *Computer Communication Review*, vol. 23, pp. 289, 1993.

[81] R. Fracchia, C. Casetti, C. F. Chiasserini, and M. Meo, "WiSE: Best-Path Selection in Wireless Multihoming Environments," *Ieee Transactions On Mobile Computing*, vol. 6, pp. 1130-1141, 2007.

[82] M. Antonio Capone, IEEE, Luigi Fratta, Fellow, IEEE, and Fabio Martignon, Student Member, IEEE, "Bandwidth Estimation Schemes for TCP over Wireless Networks," *IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 3, NO. 2, APRIL-JUNE 2004*, pp. 129-143, 2004.

[83] V. Tsaoussidis and S. Wei, *QoS Management at the Transport Layer*: IEEE Computer Society, 2000.

[84] Y. Taewan and L. Seungyun, "An approach on making use Multiple Interface of Mobile node simultaneously," presented at ICACT, Feb 2007.

[85] R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin, "Resource reSerVation Protocol (RSVP) version 1 functional specification," Sep. 1997.

[86] A. Alukdar, B. Badrinath, and A. Acharya, "MRSVP: A resource reservation protocol for an Integrated Services Packet Networks with Mobile hosts," *Wireless Net., 7:5-19*, Jan. 2001.